

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年6月7日 (07.06.2001)

PCT

(10) 国際公開番号
WO 01/41359 A1

- (51) 国際特許分類⁷: H04L 9/32,
G06F 12/14, G10K 15/02, G06F 13/00
- (21) 国際出願番号: PCT/JP00/08497
- (22) 国際出願日: 2000年12月1日 (01.12.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願平11/345244 1999年12月3日 (03.12.1999) JP
- (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ピーエフユー (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町宇宇野気ヌ98番

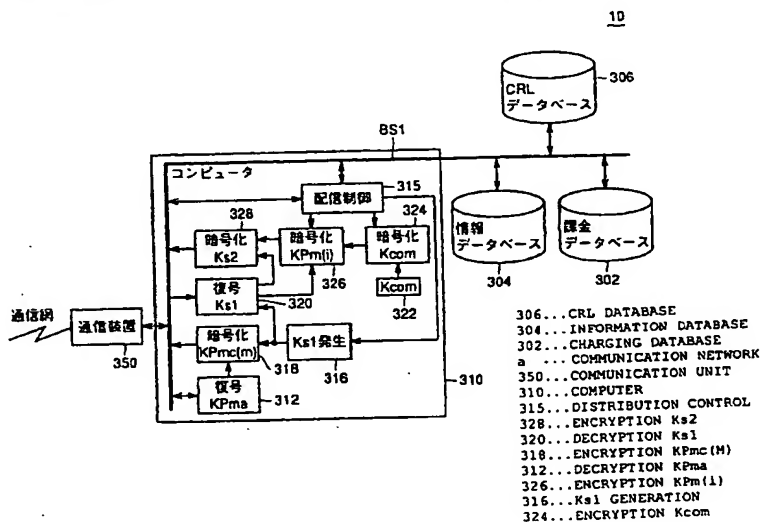
地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 吉川隆敏 (YOSHIKAWA, Takatoshi) [JP/JP]. 武村浩司 (TAKEMURA, Hiroshi) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政孝 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町宇宇野気ヌ98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 古田茂樹 (FURUTA, Shigeki) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa)

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN

(54) 発明の名称: データ配信システムおよびそれに用いられる記録装置



(57) Abstract: A license server (10) comprises a CRL database (306) for holding a prohibition list containing a specified class for which distribution, reproduction, and transfer of content data are prohibited among predetermined classes corresponding to a storage device, e.g. a memory card, and a content reproducing circuit, e.g. a portable telephone. A distribution control section (315) stops distribution if the destination class is contained in the prohibition list when the content data is distributed. The prohibition list is also held in the memory card, and the distribution control section (315) also transmits information for updating the prohibition list in the memory card when the content is distributed.

[続葉有]

BEST AVAILABLE COPY

WO 01/41359 A1



[JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP).

(74) 代理人: 深見久郎, 外(FUKAMI, Hisao et al.) ; 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,

LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

ライセンスサーバ(10)は、記憶装置たとえばメモリカードである記憶装置および、たとえば形態電話機であるコンテンツ再生回路にそれぞれ対応して予め定められるクラスのうちの、コンテンツデータの配信、再生および移動の禁止対象とされる特定のクラスを記録する禁止リストを保持するCRLデータベース(306)を備える。配信制御部(315)は、コンテンツデータの配信時において、配信先のクラスが禁止リストに含まれる場合は配信動作を中止する。禁止リストは、メモリカード内にも保持され、配信制御部(315)は、コンテンツ配信時において、メモリカード内の禁止リストを更新するための情報を併せて送信する。

明細書

データ配信システムおよびそれに用いられる記録装置

5 技術分野

本発明は、携帯電話機等の端末に対して情報を配送するためのデータ配信システムに関し、さらに詳しくは、コピーされた情報に対する著作権保護を可能とするデータ配信システムおよび当該システムで用いられメモリカードに関する。

10 背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとりて考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に

止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

5 しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化のほとんどないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDにコピーすることは、著作権保護のために機器の構成上できないようになっている。

10 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

 この場合、情報通信網を通じて公衆に送信されるコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

15 発明の開示

 この発明の目的は、情報通信網、たとえば携帯電話機等の情報通信網を介してコンテンツデータを配信することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

20 この発明の他の目的は、配信されたコンテンツデータが、著作権者の許可なく複製されることを防止することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

 この発明に従うと、データ配信システムは、複数の端末と、コンテンツ供給装置とを備える。各端末は、外部との間でデータを授受するための第1のインタフェース部と、少なくともライセンスキーを受けて記録する配信データ解読部とを
25 含む。配信データ解読部は、認証鍵によって復号することで認証可能な状態に暗号化された、配信データ解読部に対応して定められる第1のクラス証明データを保持し、ライセンスキーを受信する場合に、第1のインタフェース部を介して出力する第1の認証データ保持部と、暗号化コンテンツデータおよびライセンスキ

ーを記録するための第1の記憶部とを有する。コンテンツ供給装置は、外部との間でデータを授受するための第2のインタフェース部と、認証鍵によって復号することで正当性を証明できる状態に暗号化された第1のクラス証明データを第2のインタフェース部から受け取って、認証鍵によって復号して正当性を確認するための第1の認証処理部と、配信の禁止対象となされる第1のクラス証明データをリストアップした禁止クラスリストを保持するための禁止クラスリスト保持部と、第1の認証処理部において得られた第1のクラス証明データが禁止クラスリスト保持部に保持される禁止クラスリストに含まれる場合には、少なくともコンテンツキーの配信動作を中止する配信制御部とを含む。

好ましくは、各端末は、コンテンツ再生部をさらに含む。コンテンツ再生部は、配信データ解読部からライセンスキーと暗号化コンテンツデータとを受けて、ライセンスキーにより暗号化コンテンツデータを復号して再生するコンテンツデータ再生部と、認証鍵によって復号することで正当性が証明できる状態に暗号化された、コンテンツ再生部に対応して予め定められる、第2のクラス証明データを保持する第2の認証データ保持部とを有し、第1の認証処理部は、暗号化された第2のクラス証明データを、第2のインタフェース部から受け取って復号処理を行なう。禁止クラスリスト保持部に保持された禁止クラスリストは、禁止対象とされる第2のクラス証明データをさらにリストアップする。配信動作において、各端末は、暗号化された第2のクラス証明データを第1のインタフェース部を介して第2のインタフェース部に対して出力する。配信制御部は、第2のインタフェース部を介して入力され、第1の認証処理部によって復号された第2のクラス証明書データが、禁止クラスリスト保持部に保持される禁止クラスリストに含まれる場合には、配信動作を中止する。

このような、データ配信システムにおいては、配信動作において、配信データ解読部（メモリカード）およびコンテンツ再生部（携帯電話機）の少なくとも一方のクラスを確認して、クラスごとに配信動作を禁止することが可能である。したがって、たとえば、固有鍵が破られたクラスに対しては、配信動作を実行できないようにすることができる。この結果、正規の著作権を保護できる記録装置や再生装置を持つユーザのみがコンテンツデータを受信してメモリカード中に格納

し、復号して利用することが可能となり、かつ無制限なコピーによって著作権者が不当な不利益を被ることを防止することが可能となる。

この発明の別の局面に従うと、記録装置は、第1の記憶部と、認証処理部と、第2の記憶部と、制御部とを備える。第1の記憶部は、データを記録する。認証
5 処理部は、インタフェース部を介して入力される、認証鍵によって復号することで認証可能な状態に暗号化された第1のクラス証明データを受けて、認証鍵による復号を行なって正当性を確認する。第2の記憶部は、データの出力を禁止する対象となされる第1のクラス証明データをリストアップした禁止クラスリスト
10 (CRL) を保持する。制御部は、外部からのデータの出力指示に応じて、インタフェース部を介してデータの出力を指示する。制御部は、出力指示とともに外部からインタフェース部を介して入力される、暗号化がなされた第1のクラス証明データを認証処理部で復号して得られる第1のクラス証明データが禁止クラスリストに含まれる場合には、データの出力を中止する。

好ましくは、記録装置は、認証鍵によって復号可能な状態に暗号化された、記録装置に対応して定められる第2のクラス証明データを保持する認証データ保持
15 部をさらに備える。認証データ保持部は、外部からのデータの入力指示に応じて、認証データ保持部に保持される、認証鍵によって復号することで正当性を証明できる状態に暗号化された第2のクラス証明データをインタフェース部を介して出力する、

20 このような、記録装置においては、ライセンスキー等のデータの入出力時において、データの出力先あるいは記録装置自身のクラスを確認して、クラスごとに入出力動作の実行を禁止することが可能である。したがって、たとえば、固有鍵が破られたクラスに対しては、データの入出力を実行できないようにすることができる。この結果、正規の著作権を保護できる記録装置や再生装置を持つ正規の
25 ユーザのみがデータを受信して記録装置中に格納し、復号して利用することが可能となり、かつ無制限なコピーによって著作権者が不当な不利益を被ることを防止することが可能となる。

図面の簡単な説明

図 1 は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図 2 は、実施の形態 1 に従うデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

5 図 3 は、実施の形態 1 に従うデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

図 4 は、実施の形態 1 に従うデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

図 5 は、図 1 に示されたライセンスサーバの構成を示す概略ブロック図である。

10 図 6 は、図 1 に示された携帯電話機の構成を示す概略ブロック図である。

図 7 は、図 6 に示されたメモ리카ードの構成を示す概略ブロック図である。

図 8 は、実施の形態 1 に従うデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

15 図 9 は、実施の形態 1 に従うデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

図 10 は、実施の形態 1 に従う携帯電話機内において暗号化コンテンツデータを復号化し、音楽として外部に出力するための再生動作を説明するフローチャートである。

20 図 11 は、実施の形態 1 に従う 2 つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するための第 1 のフローチャートである。

図 12 は、実施の形態 1 に従う 2 つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するための第 2 のフローチャートである。

25 図 13 は、実施の形態 2 に従うデータ配信システムのライセンスサーバの構成を示す概略ブロック図である。

図 14 は、実施の形態 2 に従うデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

図 15 は、実施の形態 2 に従うデータ配信システムにおける配信動作を説明す

るためのフローチャートである。

図 1 6 は、実施の形態 2 に従う携帯電話機における再生動作を説明するフローチャートである。

5 図 1 7 は、実施の形態 2 に従うデータ配信システムにおける 2 つのメモリカード間の移動動作を説明するための第 1 のフローチャートである。

図 1 8 は、実施の形態 2 に従うデータ配信システムにおける 2 つのメモリカード間における移動処理を説明する第 2 のフローチャートである。

図 1 9 は、実施の形態 3 に従うメモリカードの構成を説明する概略ブロック図である。

10 図 2 0 は、実施の形態 3 に従うデータ配信システムで使用される鍵データ等をまとめて説明する図である。

図 2 1 は、実施の形態 3 に従うデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

15 図 2 2 は、実施の形態 3 に従うデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

図 2 3 は、実施の形態 3 のデータ配信システムにおいて、携帯電話機 1 1 0 における再生動作を説明するフローチャートである。

図 2 4 は、実施の形態 3 に従う 2 つのメモリカード間におけるデータ等の移動処理を説明する第 1 のフローチャートである。

20 図 2 5 は、実施の形態 3 に従う 2 つのメモリカード間におけるデータ等の移動処理を説明する第 2 のフローチャートである。

発明を実施するための最良の形態

25 以下、この発明の実施の形態によるデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

本発明の実施の形態では、携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下

の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、たとえば画像情報等のコンテンツデータを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

(実施の形態 1)

- 5 図 1 を参照して、著作権の存在する音楽データを管理するライセンスサーバ 10 は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア 20 である携帯電話会社に、このような暗号化コンテンツデータを与える。一方、認証サーバ 12 は、音楽データの配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機およびメモリ
- 10 カード等が正規の機器であるか否かの認証を行なう。

- 配信キャリア 20 は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ 10 に中継する。ライセンスサーバ 10 は、配信リクエストがあると、認証サーバ 12 により携帯電話ユーザの携帯電話機およびメモリカード等が正規の機器であることを確認し、要求されたコ
- 15 ンテンツデータをさらに暗号化した上で配信キャリア 20 の携帯電話網を介して、各携帯電話ユーザの携帯電話機に対してコンテンツデータを配信する。

- 図 1 においては、たとえば携帯電話ユーザ 1 の携帯電話機 100 には、着脱可能なメモリカード 110 が装着される構成となっている。メモリカード 110 は、携帯電話機 100 により受信された暗号化コンテンツデータを受取って、上記配
- 20 信にあたって行なわれた暗号化については復号した上で、携帯電話機 100 中の音楽再生部（図示せず）に与える。

さらに、たとえば携帯電話ユーザ 1 は、携帯電話機 100 に接続したヘッドホン 130 等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

- 25 以下では、このようなライセンスサーバ 10 と認証サーバ 12 と配信キャリア 20 と併せて、配信サーバ 30 と総称することにする。

また、このような配信サーバ 30 から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモリカード 110 を利用しないと、配

信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

5 しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

10 しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

15 このとき、たとえばメモ리카ード112を有する携帯電話ユーザ2が自己の携帯電話機102により、配信サーバ30から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等を携帯電話ユーザ2が直接配信サーバ30から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けている携帯電話ユーザ1から、そのコンテンツデータをコピーできることを可能としておけば、携帯電話ユーザにとっての利便性が向上する。

20 図1に示すように、携帯電話ユーザ1が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、携帯電話ユーザ2に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合に、携帯電話機100および102を介して、メモ리카ード110と112との間で暗号化されたコンテンツデータ（音楽データ）および再生のために必要な情報（再生情報）が移動される。ここで、「再生情報」とは、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、著作権保護にかかわる情報であるライセンスIDやアクセス再生に関する制限情報等とを有する。

 このような構成とすることによって、一旦配信サーバ30より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機 100 および 102 が PHS (Personal Handy Phone) である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、携帯電話ユーザ 1 と携帯電話ユーザ 2 との間における情報の移動を行なうことが可能である。

- 5 図 1 に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、通信における暗号鍵を配信するための方式であり、さらに第 2 には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第 3 には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

- 10 本発明の実施の形態においては、特に、配信、再生および移動の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

15 図 2 には、図 1 に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性が示される。

- 20 まず、配信サーバより配信されるデータについて説明する。Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data には、ライセンスキー Kc で復号可能な暗号化が施される。ライセンスキー Kc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc がこの形式で配信サーバ 30 より携帯電話ユーザに配布される。

 なお、以下においては、{Y} X という表記は、データ Y を、復号鍵 X により復号可能な暗号化を施したことを示すものとする。

- 25 さらに、配信サーバからは、暗号化コンテンツデータとともに、コンテンツデータに関するあるいはサーバアクセスに関する平文情報としての付加情報 Data-inf が配布される。また、再生情報としては、ライセンスキー Kc の他に、コンテンツデータ Data を識別するためのコードであるコンテンツ ID およびライセンスの発行を特定できる管理コードであるライセンス ID や、利用者側からの指定に

よって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件 AC に基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 AC 1 および再生回路における制御情報である再生回路制御情報 AC 2 等が存在する。なお、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 を総括してライセンス情報と称し、このライセンス情報とライセンスキー Kc および再生回路制限情報 AC 2 を総括して再生情報とも称する。

次に図 3 を用いて、実施の形態 1 に従うデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する。

本発明の実施の形態においては、記録装置（メモ리카ード）やコンテンツ再生回路（携帯電話機）のクラスごとに、コンテンツデータの配信、再生および移動を禁止することができるように禁止クラスリスト CRL（Class Revocation List）の運用を行なう。以下では、必要に応じて記号 CRL によって禁止クラスリスト内のデータを表わすこともある。

禁止クラスリスト関連情報には、ライセンスの配信、再生および移動が禁止されるコンテンツ再生回路およびメモ리카ードのクラスをリストアップした禁止クラスリストデータ CRL が含まれる。

禁止クラスリストデータ CRL は、配信サーバ内で管理されるとともに、メモ리카ード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データ CRL_dat の配信サーバ側より発生して、これに応じてメモ리카ード内の禁止クラスリスト CRL が書替えられる構成とする。また、禁止クラスリストのバージョンについては、CRL_ver をメモ리카ード側より出力し、これを配信サーバ側で確認することによってバージョン管理を実行する。また、禁止クラスリストのバージョンに代えて、禁止クラスリストの更新日時のような時間情報を用いても同様に運用することが可能である。

このように、禁止クラスリスト CRL を、配信サーバのみならずメモ리카ード内においても保持運用することによって、クラス固有すなわちコンテンツ再生回路およびメモ리카ードの種類に固有の復号鍵の破られた、コンテンツ再生回路およびメモ리카ードへのライセンスキーの供給を禁止する。このため、コンテンツ

再生回路ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

5 このように、メモリカード内の禁止クラスリスト CRL は配信時に逐次データを更新する構成とする。また、メモリ回路内における禁止クラスリスト CRL の管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール (Tamper Resistant Module) に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータ CRL を改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

10 コンテンツ再生回路 (携帯電話機) およびメモリカードにはクラス固有の公開暗号鍵 $KPp(n)$ および $KPmc(m)$ がそれぞれ設けられる。公開暗号鍵 $KPp(n)$ および $KPmc(m)$ はコンテンツ再生回路 (携帯電話機) のクラス固有の秘密復号鍵 $Kp(n)$ およびメモリカードのクラス固有の秘密復号鍵 $Kmc(m)$ によってそれぞれ復号可能である。クラスとは、製造会社、種類、製造時のロットなどによって区別される、公開暗号鍵 $KPmc(m)$ または $KPp(n)$ を共有する単位である。これらの公開暗号鍵および秘密復号鍵は、携帯電話機のクラスごとおよびメモリカードのクラスごとに異なる値を持つ。

20 また、メモリカードおよび再生回路のクラス証明書として、 $Cp(n)$ および $Cmc(m)$ がそれぞれ設けられる。ここで、自然数 m はメモリカードの、自然数 n はコンテンツ再生回路 (携帯電話機) のクラスを区別するための番号を表わす。これらのクラス証明書は、メモリカードおよびコンテンツ再生部 (携帯電話機) のクラスごとに異なる情報を有する。クラス固有の公開暗号鍵による暗号が破られた、すなわち、クラス固有の秘密復号鍵が漏洩したクラスは、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

25 これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ $\{KPmc(m) // Cmc(m)\} KPma$ および $\{KPp(n) // Cp(n)\} KPma$ の形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。KPma は配信システム全体で共通の認証鍵である。認証鍵 KPma を用いて、認証データ復号を行なうと、その復号結果から認証データの正当性が確認

できる。言い換えれば、認証鍵 KP_{ma} は、クラス固有の公開暗号鍵およびその証明書であるクラス証明書を承認するために用いられる鍵である。なお、認証データを作成するための暗号化は、認証鍵と対をなす非対称な秘密鍵によって行なわれる。

- 5 次に図 4 を用いて、図 1 に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する。

メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、再生および移動が行なわれるごとにサーバ 30、携帯電話機 100 または 102、メモリカード 110 または 112 において生成される共通鍵 $Ks1 \sim Ks4$ が用いられる。

ここで、共通鍵 $Ks1 \sim Ks4$ は、サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 $Ks1 \sim Ks4$ を「セッションキー」とも呼ぶこととする。

- 15 これらのセッションキー $Ks1 \sim Ks4$ は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキー $Ks1$ は、配信サーバによって配信セッションごとに発生される。セッションキー $Ks2$ は、メモリカードによって配信セッションおよび移動（受信側）セッションごとに発生し、セッションキー $Ks3$ は、
20 同様にメモリカードにおいて再生セッションおよび移動（送信側）セッションごとに発生する。セッションキー $Ks4$ は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションに
25 おけるセキュリティ強度を向上させることができる。

また、メモリカード 100 内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵 $KP_m(i)$ (i : 自然数) と、公開暗号鍵 $KP_m(i)$ で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 $Km(i)$ が存在する。ここで、自然数 i は、各メモリカー

ドを区別するための番号を表わす。

その他の鍵としては、システムに共通の秘密鍵として、主としてライセンスキーKcの取得に利用される共通鍵方式における秘密鍵Kcomが存在する。秘密鍵Kcomは、配信サーバおよび携帯電話機の双方において保持され、ライセンスキーKc等の暗号化および取得のための復号処理にそれぞれ使用される。

なお、共通鍵方式における秘密鍵Kcomを、公開鍵方式における公開暗号鍵Kpcomおよび秘密復号鍵Kcomの組に置き換えて運用することも可能である。この場合には、公開暗号鍵Kpcomは配信サーバに保持されてライセンスキーKcの暗号化に使用され、秘密復号鍵Kcomは、携帯電話機に保持されてライセンスキーKcの取得に使用される。

図5を参照して、ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベース304、課金データベース302およびCRLデータベース306からのデータをデータベースBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

データ処理部310は、データベースBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモ리카ードおよび携帯電話機から送られてきた認証データ{KPmc(m) // Cmc(m)} KPmaおよび{KPp(n) // Cp(n)} KPmaを通信装置350およびデータベースBS1を介して受けて、KPmaによる復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵KPmc(m)を用いて暗号化して、データベースBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをデータベースBS1を

より受けて、復号処理を行なう復号処理部 320 とを含む。

データ処理部 310 は、さらに、再生回路に共通な秘密鍵 Kcom を保持する Kcom 保持部 322 と、配信制御部 315 から与えられるライセンスキー Kc および再生回路制御情報 AC2 を再生回路共通の秘密鍵 Kcom で暗号化する暗号化処理部 324 と、暗号化処理部 324 から出力されたデータを復号処理部 320 によって得られたメモリカード固有の公開暗号鍵 Kpm (i) によって暗号化するための暗号化処理部 326 と、暗号化処理部 326 の出力を、復号処理部 320 から与えられるセッションキー Ks2 によってさらに暗号化してデータバス BS1 に出力するための暗号化処理部 328 とを含む。

なお、共通鍵 Kcom に代えて公開鍵方式における公開暗号鍵 Kpcom および秘密復号鍵 Kcom の組を用いる場合には、Kcom 保持部 322 に相当する部分に公開暗号鍵 Kpcom が保持される。さらに、暗号化処理部 324 によって、公開暗号鍵 Kpcom による暗号化が行なわれる。

ライセンスサーバ 10 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図 6 を参照して、携帯電話機 100 においては、携帯電話機のクラスを表わす自然数 $n = 1$ 、携帯電話機を個別に識別する自然数 $i = 1$ とする。

携帯電話機 100 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス BS2 と、データバス BS2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 とを含む。

携帯電話機 100 は、さらに、外部からの指示を携帯電話機 100 に与えるためのタッチキー部 1108 と、コントローラ 1106 等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データベース BS2 を介して与えられる受信データに基づいて音声再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス BS

2に与え得る信号に変換し、または、データベース BS 2からのデータをコネクタ 1 1 2 0に与え得る信号に変換するための外部インタフェース部 1 1 2 2とを含む。

5 携帯電話機 1 0 0は、さらに、配信サーバ 3 0からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード 1 1 0と、メモリカード 1 1 0とデータベース BS 2との間のデータの授受を制御するためのメモリインタフェース 1 2 0 0と、携帯電話機のクラスごとにそれぞれ設定される公開暗号鍵 KPp (1) およびクラス証明書 Cp (1) を認証鍵 KPma で復号することで認証可能な状態に暗号化したデータを保持する認証データ保持部 1 5 0 0
10 を含む。

携帯電話機 1 0 0は、さらに、携帯電話機（コンテンツ再生回路）のクラス固有の秘密復号鍵である Kp (1) を保持する Kp 保持部 1 5 0 2と、データベース BS 2から受けたデータを Kp (1) によって復号しメモリカードによって発生されたセッションキーKs 3を得る復号処理部 1 5 0 4と、メモリカード 1 1 0に
15 記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード 1 1 0との間でデータベース BS 2上においてやり取りされるデータを暗号化するためのセッションキーKs 4を乱数等により発生するセッションキー発生部 1 5 0 8と、生成されたセッションキーKs 4を復号処理部 1 5 0 4によって得られたセッションキーKs 3によって暗号化しデータベース BS 2に出力する暗号化処理部 1 5 0 6と、データベース BS 2上のデータをセッションキーKs 4によって復号して出力する復号処理部 1 5 1 0とをさらに含む。

携帯電話機 1 0 0は、さらに、再生回路に共通に設定される秘密鍵 Kcom を保持する Kcom 保持部 1 5 1 2と、復号処理部 1 5 1 0が出力する {Kc//AC 2} Kcom を秘密鍵 Kcom で復号しライセンスキーKc および再生回路制御情報 AC 2
25 を出力する復号処理部 1 5 1 4と、データベース BS 2より暗号化コンテンツデータ {Data} Kc を受けて、復号処理部 1 5 1 4より取得してライセンスキーKc によって復号しコンテンツデータを出力する復号処理部 1 5 1 6と、復号処理部 1 5 1 6の出力を受けてコンテンツデータを再生するための音楽再生部 1 5 1 8と、音楽再生部 1 5 1 8と音声再生部 1 1 1 2の出力を受けて、動作モードに応じて

選択的に出力するための切換部 1 5 2 5 と、切換部 1 5 2 5 の出力を受けて、ヘッドホン 1 3 0 と接続するための接続端子 1 5 3 0 とを含む。

なお、図 6 においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックに付いては、一部記載を省略している。

また、携帯電話ユーザの利便性を図るために、携帯電話機 1 0 0 のうち、通話処理に関するブロックを除いた、図 6 において点線で囲まれる、コンテンツデータの配信および再生に関するブロック全体を音楽再生モジュール 1 5 5 0 として、着脱可能なモジュール化する構成を採用することも可能である。

なお、共通鍵 Kcom に代えて公開鍵方式における公開暗号鍵 Kpcom および秘密復号鍵 Kcom の組を用いる場合には、Kcom 保持部 1 5 1 2 に相当する部分に秘密復号鍵 Kcom が保持される。さらに、復号処理部 1 5 1 4 によって、秘密復号鍵 Kcom による復号化が行なわれる。

携帯電話機 1 0 0 の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図 7 を参照して、公開暗号鍵 KPm (i) およびこれに対応する秘密復号鍵 Km (i) は、メモ리카ードごとに固有の値であるが、メモ리카ード 1 1 0 においては、この自然数 i=1 として取扱う。また、メモ리카ードのクラス固有の公開暗号鍵および秘密復号鍵として、KPmc (m) および Kmc (m) が設けられ、メモ리카ードのクラス証明書として Cmc (m) が設けられるが、メモ리카ード 1 1 0 においては、これらは自然数 m=1 でそれぞれ表わされるものとする。

したがって、メモ리카ード 1 1 0 は、認証データ {KPmc (1) //Cmc (1)} KPma を保持する認証データ保持部 1 4 0 0 と、メモ리카ードのクラスごとに設定される固有の復号鍵である Kmc (1) を保持する Kmc 保持部 1 4 0 2 と、メモ리카ードごとに固有に設定される秘密復号鍵 Km (1) を保持する Km (1) 保持部 1 4 2 1 と、Km (1) によって復号可能な公開暗号鍵 KPm (1) を保持する KPm (1) 保持部 1 4 1 6 とを含む。

このように、メモ리카ードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたラ

メモリカード110は、さらに、メモリインタフェース1200との間で信号

5

15

25

納するためのメモリ 1415 とを含む。メモリ 1415 は、例えば半導体メモリによって構成される。

メモリカード 110 は、さらに、配信サーバより与えられる禁止クラスリストのバージョン更新のための差分データ CRL_dat によって逐次更新される禁止クラスリスト CRL を格納するための CRL 保持部 1430 と、復号処理部 1422 によって得られるライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 を保持するためのライセンス情報保持部 1440 と、データベース BS3 を介して外部との間でデータ授受を行ない、データベース BS4 との間で再生情報等を受けて、メモリカード 110 の動作を制御するためのコントローラ 1420 とを含む。

ライセンス情報保持部 1440 は、データベース BS4 との間で、ライセンス情報（コンテンツ ID、ライセンス ID、アクセス制御情報 AC1）の授受が可能である。ライセンス情報保持部 1440 は、N 個（N：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

なお、図 7 において、実線で囲んだ領域は、メモリカード 110 内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール TRM に組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュールが用いられる。

もちろん、メモリ 1415 も含めて、モジュール TRM 内に組込まれる構成としてもよい。しかしながら、図 7 に示したような構成とすることで、メモリ 1415 中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ 1415 中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ 1415 を設ける必要がないので、製造コストが低減されるという利点がある。

しかしながら、十分な TRM 領域が確保できるのであれば、ライセンス保持部 1440 に、復号して平文となったすべての再生情報（ライセンスキー Kc、再生回路制御情報 AC2、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1）を保持しても問題はなく、同様な効果を得ることができる。

次に、本発明の実施の形態 1 に従うデータ配信システムの各セッションにおけ

これらの公開暗号鍵が無効である場合には、処理を終了（ステップS 1 7 0）する（ステップS 1 1 0）。

また、認証データ {KPmc (1)} KPma (および認証データ {KPp (1)}) KPma は、それぞれが認証鍵 KPma によって復号することで、その正当性が判断
5 可能な暗号化が施されているため、認証サーバ 1 2 に対して照会せず、ライセンスサーバ 1 0 の配信制御部 3 1 5 が、認証鍵 KPma による復号結果から独自に認証を行なう構成としてもよい。

照会の結果、正規の機器であることが認識されると、配信制御部 3 1 5 は、次に、メモリカード 1 1 0 および携帯電話機 1 0 0 のコンテンツ再生回路のクラス
10 証明書 Cmc (1) および Cp (1) が禁止クラスリスト CRL にリストアップされているかどうかを CRL データベース 3 0 6 に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップS 1 7 0）。

一方、メモリカード 1 1 0 および携帯電話機 1 0 0 の再生回路のクラス証明書
15 が禁止クラスリストの対象外である場合には次の処理に移行する（ステップS 1 1 2）。

照会の結果、正規のクラス証明書を持つメモリカードと再生回路とを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ 3 0 において、セッションキー発生部 3 1 6 は、配
20 信のためのセッションキー Ks 1 を生成する。セッションキー Ks 1 は、復号処理部 3 1 2 によって得られたメモリカード 1 1 0 に対応する公開暗号鍵 KPmc (1) によって、暗号化処理部 3 1 8 によって暗号化される（ステップS 1 1 4）。

暗号化されたセッションキー Ks 1 は、{Ks 1} Kmc (1) として、データベース BS 1 および通信装置 3 5 0 を介して外部に出力される（ステップS 1 1 6）。

携帯電話機 1 0 0 が、暗号化されたセッションキー {Ks 1} Kmc (1) を受信すると（ステップS 1 1 8）、メモリカード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データベース BS 3 に与えられた受信データを、復号処理部 1 4 0 4 が、保持部 1 4 0 2 に保持されるメモリカード 1 1 0 固有の秘密復

号鍵 Kmc (1) により復号処理することにより、セッションキー Ks1 を復号し抽出する (ステップ S120)。

5 コントローラ 1420 は、配信サーバ 30 で生成されたセッションキー Ks1 の受理を確認すると、セッションキー発生部 1418 に対して、メモ리카ードにおいて配信動作時に生成されるセッションキー Ks2 の生成を指示する。

また、配信セッションにおいては、コントローラ 1420 は、メモ리카ード 110 内の CRL 保持部 1430 に格納されている禁止クラスリストの状態 (バージョン) に関連する情報として、リストのバージョンデータ CRL_ver を CRL 保持部 1430 から抽出してデータバス BS4 に出力する。

10 暗号化処理部 1406 は、切換スイッチ 1442 の接点 Pa を介して復号処理部 1404 より与えられるセッションキー Ks1 によって、切換スイッチ 1444 および 1446 の接点を順次切換えることによって与えられるセッションキー Ks2、公開暗号鍵 Kpm (1) および禁止クラスリストのバージョンデータ CRL_ver を 1 つのデータ列として暗号化して、{Ks2//Kpm (1) //CRL_ver} Ks1
15 1 をデータバス BS3 に出力する (ステップ S122)。

データバス BS3 に出力された暗号データ {Ks2//Kpm (1) //CRL_ver} Ks1 は、データバス BS3 から端子 1202 およびメモリインタフェース 1200 を介して携帯電話機 100 に出力され、携帯電話機 100 から配信サーバ 30 に送信される (ステップ S124)。

20 配信サーバ 30 は、暗号化データ {Ks2//Kpm (1) //CRL_ver} Ks1 を受信して、復号処理部 320 においてセッションキー Ks1 による復号処理を実行し、メモ리카ード 110 で生成されたセッションキー Ks2、メモ리카ード 110 固有の公開暗号鍵 Kpm (1) およびメモ리카ード 110 における禁止クラスリストのバージョンデータ CRL_ver を受理する (ステップ S126)。

25 禁止クラスリストのバージョン情報 CRL_ver は、データバス BS1 を介して配信制御部 315 に送られ、配信制御部 315 は、受理したバージョンデータ CRL_ver に従って、当該 CRL_ver のバージョンと CRL データベース 306 内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データ CRL_dat を生成する (ステップ S128)。

さらに、配信制御部 3 1 5 は、ステップ S 1 0 6 で取得したコンテンツ ID およびライセンス購入条件 AC に従って、ライセンス ID、アクセス制限情報 AC 1 および再生回路制御情報 AC 2 を生成する（ステップ S 1 3 0）。さらに、暗号化コンテンツデータを復号するためのライセンスキー Kc を情報データベース 3 0 4 より取得する（ステップ S 1 3 2）。

図 9 を参照して、配信制御部 3 1 5 は、取得したライセンスキー Kc および再生回路制御情報 AC 2 を暗号化処理部 3 2 4 に与える。暗号化処理部 3 2 4 は、Kcom 保持部 3 2 2 より得られる、秘密鍵 Kcom によって、ライセンスキー Kc および再生回路制御情報 AC 2 を暗号化する（ステップ S 1 3 4）。

暗号化処理部 3 2 4 が出力する暗号化データ {Kc//AC 2} Kcom と、配信制御部 3 1 5 が出力するライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 とは、暗号化処理部 3 2 6 によって、復号処理部 3 2 0 によって得られたメモリカード 1 1 0 固有の公開暗号鍵 KPm (1) によって暗号化される（ステップ S 1 3 6）。暗号化処理部 3 2 8 は、暗号化処理部 3 2 6 の出力と、配信制御部 3 1 5 が出力する禁止クラスリストのバージョンの更新情報 CRL_dat とを受けて、メモリカード 1 1 0 において生成されたセッションキー Ks 2 によって暗号化する。暗号化処理部 3 2 8 より出力された暗号化データは、データベース BS 1 および通信装置 3 5 0 を介して携帯電話機 1 0 0 に送信される（ステップ S 1 3 8）。

このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号データを相手方に送信することによって、それぞれの暗号データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

携帯電話機 1 0 0 は、送信された暗号化データ { { { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC 1} Km (1) //CRL_dat} Ks2 を受信し（ステップ S 1 4 0）、メモリカード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データベース BS 3 に与えられた受信データを復号処理部 1 4 1 2 によって復号する。復号処理部 1 4 1 2 は、セッションキー発生部 1 4 1 8 から与え

られたセッションキーKs2を用いてデータベース BS3の受信データを復号しデータベース BS4に出力する(ステップS142)。

この段階で、データベース BS4には、Km(1)保持部1421に保持される秘密復号鍵 Km(1)で復号可能な暗号化再生情報{ {KC//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(1)と、CRL_dat とが出力される。コントローラ1420の指示によって、暗号化再生情報{ {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(1)は、メモリ1415に記録される(ステップS144)。一方、{ {KC//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(1)は、復号処理部1422において、秘密復号鍵 Km(1)によって復号され、ライセンス情報であるライセンス ID、コンテンツ ID およびアクセス制限情報 AC1のみが受理される(ステップS146)。

コントローラ1420は、受理した CRL_dat に基づいて、CRL 保持部1430内の禁止クラスリストデータ CRL およびそのバージョンを更新する(ステップS148)。さらに、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1については、ライセンス情報保持部1440に記録される(ステップS150)。

ステップS150までの処理がメモリ回路で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる(ステップS152)。

配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ {Data} Kc および付加情報 Data-infを取得して、これらのデータをデータベース BS1および通信装置350を介して出力する(ステップS154)。

携帯電話機100は、{Data} Kc//Data-infを受信して、暗号化コンテンツデータ {Data} Kc および付加情報 Data-infを受理する(ステップS156)。暗号化コンテンツデータ {Data} Kc および付加情報 Data-infはメモリインタフェース1200および端子1202を介してメモリカード110のデータベース BS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ {Data} Kc および付加情報 Data-infがそのままメモリ1415に記録される(ス

ステップS158)。

さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され(ステップS160)、配信サーバ30で配信受理を受信すると(ステップS162)、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され(ステップS164)、全体の処理が終了する(ステップS170)。

このようにして、携帯電話機100のコンテンツ再生部およびメモリカード110が正規の機器であること、同時に、それぞれがクラス証明書Cp(1)およびCmc(1)とともに暗号化して送信できた公開暗号鍵Kp(1)およびKmc(1)が有効であることを確認した上で、それぞれのクラス証明書Cp(1)およびCmc(1)が禁

止クラスリスト、すなわち、公開暗号鍵Kp(1)およびKmc(1)による暗号化が破られたクラス証明書リストに記載されていない機器からの配信要求に対してのみコンテンツデータを配信することができ、不正な機器および暗号化の破られた機器への配信を禁止することができる。

次に図10のフローチャートを用いて、携帯電話機100内において、メモリカード110に保持された暗号化コンテンツデータから音楽を再生し、外部に出力するための再生動作(以下、再生セッションともいう)を説明する。

図10を参照して、携帯電話機のタッチキー部1108からの携帯電話ユーザ1の指示により、再生リクエストが生成される(ステップS200)。携帯電話機100は、再生リクエストの生成に応じて、認証データ保持部1500より、認証鍵KPmaで復号することで認証可能な認証データ{KPp(1)//Cp(1)}KPmaをデータベースBS2に出力する(ステップS202)。

認証データ{KPp(1)//Cp(1)}KPmaは、データベースBS2およびメモリインタフェース1200を介してメモリカード110に伝達される。

メモリカード110においては、端子1202を介してデータベースBS3に伝達される認証データ{KPp(1)//Cp(1)}KPmaは、復号処理部1408に取込まれる。復号処理部1408は、KPma保持部1414から認証鍵KPmaを受けて、データベースBS3のデータを復号処理し、コンテンツ再生部すなわち携帯電話機100の種類に固有の公開暗号鍵Kp(1)およびクラス証明書Cp

(1)を得る。コントローラ1420は、データベースBS3を介して公開暗号鍵KPp(1)およびクラス証明書Cp(1)を受理する(ステップS204)。

5 コントローラ1420は、復号処理部1408の復号結果に基づいて、受理した携帯電話機100のコンテンツ再生回路の認証作業を行ない、携帯電話機100のコンテンツ再生回路が承認されたものである場合には処理を次のステップ(ステップS208)に進める(ステップS206)。一方、携帯電話機100のコンテンツ再生回路が非承認である場合には、再生セッションの処理を終了する(ステップS240)。

10 携帯電話機100が承認された機器であることを確認した場合には、引続き、携帯電話機100のコンテンツ再生部のクラス証明書Cp(1)が禁止クラスリストCRLにリストアップされているかの判定が実行される(ステップS208)。ステップS208においては、携帯電話機100のクラスが禁止クラスリストCRLにリストアップされているクラスに含まれる場合には、再生セッションの処理を終了する(ステップS240)。

15 一方、携帯電話機100のクラスが、禁止クラスリストCRLに含まれない場合においては、次のステップに処理を進め、コントローラ1420は、セッションキー発生部1418に対して、再生セッションにおけるセッションキーKs3の生成をデータベースBS4を介して指示する。セッションキー発生部1418によって生成されたセッションキーKs3は、暗号化処理部1410に送られる。
20 暗号化処理部1410は、復号処理部1408によって得られた携帯電話機100の公開暗号鍵KPp(1)によってセッションキーKs3を暗号化し公開暗号鍵KPp(1)に対応する秘密復号鍵Kp(1)で復号可能な暗号化データ{Ks3}Kp(1)をデータベースBS3に出力する(ステップS210)。

25 携帯電話機100は、端子1202およびメモリアンタフェース1200を介して、データベースBSに暗号化データ{Ks3}Kp(1)を受ける。暗号化データ{Ks3}Kp(1)は、復号処理部1504によって復号され、メモ리카ード110で生成されたセッションキーKs3が受理される(ステップS212)。

コントローラ1106は、セッションキーKs3の受理に応じて、セッションキー発生部1508に対して、再生セッションにおいて携帯電話機100で生成

されるセッションキーKs4の発生をデータベースBS2を介して指示する。生成されたセッションキーKs4は暗号化処理部1506に送られ、復号処理部1504によって得られたセッションキーKs3によって暗号化された{Ks4}Ks3がデータベースBS2に受理される(ステップS214)。

- 5 暗号化されたセッションキー{Ks4}Ks3は、メモリインタフェース1200を介してメモリカード110に伝達される。メモリカード110においては、データベースBS3に伝達される暗号化されたセッションキー{Ks4}Ks3を復号処理部1412によって復号し、携帯電話機で生成されたセッションキーKs4を受理する(ステップS216)。セッションキーKs4の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する(ステップS218)。
- 10 ステップS218においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生セッションを終了し(ステップS240)、再生回数に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS220)。一方、アクセス制限情報AC1によって再生回数が制限されていない場合においては、ステップS220はスキップされ、再生制御情報AC1は更新されることなく処理が次のステップ(ステップS222)に進行される。

- 15 ステップS218においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生セッションを終了し(ステップS240)、再生回数に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS220)。一方、アクセス制限情報AC1によって再生回数が制限されていない場合においては、ステップS220はスキップされ、再生制御情報AC1は更新されることなく処理が次のステップ(ステップS222)に進行される。
- 20 また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態にあると判断して、再生セッションを終了する(ステップS240)。

- 25 ステップS218において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーKcを含む再生情報の復号処理が実行される。具体的には、コントローラ1420の指示に応じて、メモリ1415からデータベースBS4に読出された暗号化再生情報({Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1)Km(1)を復号処理部1422がメモリカード110固有の秘密復号鍵Km(1)によって復号し、共通の秘密鍵Kcomによって復号可能な暗号化データ{Kc//AC2}

Kcom がデータベース BS 4 上に得られる (ステップ S 2 2 2)。

得られた暗号化データ {Kc// AC 2} Kcom は、切換スイッチ 1 4 4 4 の接点 Pd を介して暗号化処理部 1 4 0 6 に送られる。暗号化処理部 1 4 0 6 は、切換スイッチ 1 4 4 2 の接点 Pb を介して復号処理部 1 4 1 2 より受けたセッションキー Ks 4 によってデータベース BS 4 から受けた暗号化データをさらに暗号化し、
5 { {Kc//AC 2} Kcom} Ks 4 をデータベース BS 3 に出力する (ステップ S 2 2 4)。
データベース BS 3 に出力された暗号化データは、メモリインタフェース 1 2 0 0 を介して携帯電話機 1 0 0 に送出される。

携帯電話機 1 0 0 においては、メモリインタフェース 1 2 0 0 を介してデータベース BS 2 に伝達される暗号化データ { {Kc//AC 2} Kcom} Ks 4 を復号処理部 1
10 5 1 0 によって復号処理を行ない、暗号化されたライセンスキー Kc および再生回路制御情報 AC 2 を受取する (ステップ S 2 2 6)。復号処理部 1 5 1 4 は、暗号化データ {Kc//AC 2} Kcom を、Kcom 保持部 1 5 1 2 から受けた再生回路に共通の秘密鍵 Kcom によって復号し、ライセンスキー Kc および再生回路制御
15 情報 AC 2 を受取する (ステップ S 2 2 8)。復号処理部 1 5 1 4 は、ライセンスキー Kc を復号処理部 1 5 1 6 に伝達し、再生回路制御情報 AC 2 をデータベース BS 2 に出力する。

コントローラ 1 1 0 6 は、データベース BS 2 を介して、再生回路制御情報 AC 2 を受取して再生の可否の確認を行なう (ステップ S 2 3 0)。

20 ステップ S 2 3 0 においては、再生回路制御情報 AC 2 によって再生不可と判断される場合には、再生セッションは終了される (ステップ S 2 4 0)。一方、再生可能である場合には、メモリカード 1 1 0 よりメモリに記録されたリクエスト曲の暗号化されたコンテンツデータ {Data} Kc がデータベース BS 3 に出力され、メモリインタフェース 1 2 0 0 を介して携帯電話機 1 0 0 に伝達される (ステップ S 2 3 2)。
25

携帯電話機 1 0 0 においては、メモリカード 2 1 0 から出力されデータベース BS 2 に伝達された暗号化コンテンツデータ {Data} Kc を復号処理部 1 5 1 6 においてライセンスキー Kc によって復号し、平文化されたコンテンツデータ Data を得ることができる (ステップ S 2 3 4)。復号された平文化コンテンツデータ

Data は音楽再生部 1518 によって音楽信号に変換され (ステップ 230)、混合部 1525 および端子 1530 を介して外部に再生された音楽を出力することによって処理が終了する (ステップ S240)。

5 このような構成とすることで、メモ리카ード 110 側において、コンテンツ再生回路である携帯電話機 100 のクラスを確認し、禁止クラスリストにリストアップされているクラスに対しては、再生処理を禁止することが可能となる。

再生セッションにおいても、携帯電話機 100 およびメモ리카ード 110 でそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する。この結果、配信セッション
10 同様、再生セッションにおいても、データのそれぞれの送受信において事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

次に図 11 および図 12 のフローチャートを用いて、2 つのメモ리카ード 110 および 112 の間で携帯電話機 100 および 102 を介してコンテンツデータ
15 およびキーデータ等の移動を行なう処理を説明する。

図 11 および図 12 においては、携帯電話機 100 およびメモ리카ード 110 についてのクラスを識別するための自然数をそれぞれ $m=1$ および $n=1$ とし、携帯電話機 102 およびメモ리카ード 112 についてのクラスを認識するため自然数をそれぞれ $m=2$ および $n=2$ とする。また、メモ리카ード 110 および
20 112 を識別するための自然数 i は、それぞれ $i=1$ および $i=2$ であるものとする。

図 11 および図 12 においては、携帯電話機 100 およびメモ리카ード 110 が送信側であり、携帯電話機 102 およびメモ리카ード 112 が受信側であるものとする。また、携帯電話機 102 も、メモ리카ード 110 と同様の構成を有するメモ리카ード 112 が装着されているものとする。以下、メモ리카ード 112
25 の各構成部分については、メモ리카ード 110 の対応する部分と同一の符号を用いて説明する。

図 11 を参照して、まず送信側である携帯電話ユーザ 1 により、携帯電話機 100 からタッチキー部 1108 のキーボタンの操作等によって、コンテンツ移動

リクエストがなされる。(ステップS300)。

生成された移動リクエストは、受信側である携帯電話ユーザ2の携帯電話機120を介してメモリカード112に伝達される。メモリカード112においては、認証データ保持部1500より、メモリカード112に対応する公開暗号鍵 KPmc (2) およびクラス証明書 Cmc (2) が暗号化された認証データ {KPmc (2) //Cmc (2) } KPma が出力される(ステップS302)。

メモリカード112の認証データ {KPmc (2) //Cmc (2) } KPma は、携帯電話ユーザ2の携帯電話機120から送信され、携帯電話ユーザ1の携帯電話機110を経由してメモリカード110に受信される(ステップS304)。

メモリカード110においては、復号処理部1408によって、メモリカード112の認証データが復号され、メモリカード112に関する公開暗号鍵 KPmc

(2) およびクラス証明書 Cmc (2) が受理される(ステップS306)。コントローラ1420は、データバス BS3を介して受理された認証処理部1408の復号結果に基づいて、認証作業を実行する(ステップS308)。まず、コントローラ1420は、メモリカード112に関する認証データ {KPmc (2) //Cmc (2) } KPma を認証鍵 KPma によって復号した復号結果から、認証データ {KPmc (2) //Cmc (2) } KPma が正規の機器から出力された認証データであることを確認し、正規の機器から出力された有効な認証データである場合には、公開暗号鍵 KPmc (2) およびクラス証明書 Cmc (2) を承認し、次のステップ S310を実行する。正規の機器から出力されたことが確認できない無効な認証データである場合には、移動セッションを終了する(ステップS360)。

認証の結果、有効な認証データである場合には、コントローラ1420は、引き続き、メモリカード112のクラス証明書 Cmc (2) が禁止クラスリストに含まれるか否かの判定を実行する(ステップS310)。メモリカード112に関するクラス証明書 Cmc (2) が禁止クラスリストに含まれる場合においては、移動セッションはこの段階で終了される(ステップS360)。一方、メモリカード112の属するクラスが禁止クラスリストに含まれない場合においては、移動セッションを実行するために次のステップS312に処理が進行する。

この場合においては、コントローラ1420は、セッションキー発生部141

- 8に対して、移動セッション時に送信側で発生されるセッションキーKs3の出力を指示する。セッションキー発生部1418によって生成されたセッションキーKs3は、暗号化処理部1410に伝達される。暗号化処理部1410は、さらに、ステップS306において復号処理部1408によって復号されたメモリカード112の公開暗号鍵 KPmc (2) によってセッションキーKs3を暗号化する。これにより、暗号化されたセッションキー {Ks3} Kmc (2) がデータバスBS3に出力される (ステップS314)。データバスBS3に出力された {Ks3} Kmc (2) は、メモリインタフェース1200、携帯電話機100、および携帯電話機102を介してメモリカード112に伝達される。
- 10 メモリカード112は、メモリカード110から出力された {Ks3} Kmc (2) を受けて、復号処理部1404によってメモリカード112に対応する秘密復号鍵 Kmc (2) による復号処理を実行し、送信側のメモリカード110によって生成されたセッションキーKs3を受理する (ステップS316)。
- 15 メモリカード112のコントローラ1420は、セッションキーKs3の受理に応じて、セッションキー発生部1418に対して、移動セッションにおいて受信側で発生されるべきセッションキーKs2の生成を指示する。生成されたセッションキーKs2は、切換スイッチ1446中の接点 Pf および切換スイッチ1444中の接点Pcを経由して暗号化処理部1406に伝達される。
- 20 暗号化処理部1406は、復号処理部1404からステップS316で得られたセッションキーKs3を受けて、切換スイッチ1444の接点 Pc と切換スイッチ1446の接点の切換によって得られるセッションキーKs2と公開暗号鍵 KPm (2) をセッションキーKs3によって暗号化し、 {Ks2//KPm (2)} Ks3 をデータバスBS3に出力する (ステップS318)。データバスBS3に出力された暗号化データ {Ks2//KPm (2)} Ks3は、携帯電話機102および100を介してメモリカード110のデータバスBS3に伝達される。
- 25 メモリカード110においては、データバスBS3に伝達された暗号化データを符号処理部1412によってセッションキーKs3を用いて復号し、メモリカード112に関するセッションキーKs2および公開暗号鍵 KPm (2) を受理する (ステップS320)。

メモリカード110のコントローラ1420は、セッションキーKs2および公開暗号鍵 KPm (2) の受理に応じて、ライセンス情報保持部1440内のアクセス制限情報 AC1の確認を実行する。アクセス制御情報 AC1を確認した結果、ライセンスの移動が不可である場合には、この段階で移動を終了する（ステップS360）。一方、アクセス制限情報 AC1を確認した結果、移動セッションが許可されている場合には、次のステップに進み（ステップS322）、ライセンス情報保持部1440より対応するコンテンツ ID およびライセンス ID を取得し、さらにライセンス情報保持部1440内のアクセス制御情報 AC1 を更新して、以降の再生および移動の禁止を記録する（ステップS324）。これに対応して、再生セッションおよび移動セッションにおいて当該アクセス制御情報 AC1を確認して処理が行なわれ、以降のそれぞれのセッションが禁止される。

さらに、コントローラ1420は、移動するコンテンツデータに対応したセッションキーKc および再生情報に関する暗号化再生情報 { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (1) の出力をメモリ1415に対して指示する。メモリ1415から出力された暗号化再生情報 { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (1) は、復号処理部1422によって復号化され、{Kc//AC2} Kcom がデータバス BS4上に得られる（ステップS326）。

ステップS324でライセンス情報保持部1440から取得されたライセンス ID、コンテンツ ID、およびアクセス制限情報 AC1と、ステップS326で得られた {Kc//AC2} Kcom は、データバス BS4から暗号化処理部1424に取込まれて暗号化される。暗号化処理部1424は、ステップS320において復号処理部1412で得られた受信側メモリカード112固有の公開暗号鍵 KPm (2) によって、これらのデータを暗号化し、暗号化再生情報 { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (2) を出力する（ステップS328）。

図12を参照して、データバス BS4に出力された暗号化再生情報 { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (2) は、切換スイッチ1444中の接点 Pd を介して暗号化処理部1406に伝達される。暗号化処理部

1406は、復号処理部1412によって得られたメモリカード112の生成したセッションキーKs2を切換スイッチ1442の接点 Pb を介して受けて、接点 Pd より受けたデータをセッションキーKs2によって暗号化する。

5 暗号化処理部1406は、暗号化データ { { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (2) } Ks2 をデータバス BS3 に出力する (ステップ S330)。ステップ S330 においてデータバス BS3 に出力された暗号化再生情報は、携帯電話機100および102を介して、移動セッションの受信側であるメモリカード112に伝達される。

10 メモリカード112においては、復号処理部1412においてセッションキー発生部1418によって生成されたセッションキーKs2による復号が実行され、暗号化再生情報 { { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (2) } が受理される (ステップ S332)。

15 暗号化再生情報 { { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (2) } は、メモリ1415に記録される (ステップ S334)。さらに、復号処理部1422において、メモリカード112に固有の秘密復号鍵 Km (2) による復号処理を実行することにより、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 が受理される (ステップ S336)。

20 復号処理部1422によって得られたライセンス ID、およびコンテンツ ID およびアクセス制限情報 AC1 は、データバス BS4 を介してライセンス情報保持部1440に記録される (ステップ S338)。

このようにして、ステップ S338 までの処理が正常に終了することによって、ライセンスキー Kc を含む再生情報が移動されたことに応答して、携帯電話機102を介してコンテンツデータの複製要求がさらに行なわれる (ステップ S340)。

25 コンテンツデータの複製要求は携帯電話機100を経由してメモリカード110に伝達され、これに応答して、メモリカード110中のメモリ1415より対応する暗号化コンテンツデータ {Data} Kc と付加情報 Data-inf とがデータバス BS3 に出力される (ステップ S342)。

データバス BS3 に出力されたこれらのデータは、携帯電話機100および携

携帯電話機 102 を介してメモリカード 112 に伝達され、メモリカード 112 中のメモリ 1415 に記録される（ステップ S344）。

暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf の記録が終了すると、携帯電話機 102 を介して移動受理が送信される（ステップ S346）。

- 5 これにより、メモリカード 112 および対応する携帯電話機 102 において正常に再生セッションが実行されれば、携帯電話機 102 によって、メモリカード 112 に記録された暗号化コンテンツデータを再生して音楽を聴取することが可能となる。

- 10 送信側の携帯電話機 100 においては、携帯電話機 102 から送信された移動受理を受信して（ステップ S348）、コンテンツデータの消去もしくは保持のいずれかをキー 1108 より入力する（ステップ S350）。本発明の実施の形態に従うデータ配信システムにおいては、利用者のライセンス数や再生可能回数に応じて再生が可能であるか否かは、アクセス制限情報 AC1 に応じて再生セッションによって判断されるため、携帯電話機 100 側において、既に再生が不可能となった場合には、これ以上、暗号化コンテンツデータ等を保持する必要がない。

- 20 したがって、このような場合には、タッチキー部 1108 よりコンテンツデータの消去を指示することにより、メモリカード 110 内のメモリ 1415 において、対応する暗号化コンテンツデータ {Data} Kc、付加情報 Data-inf を消去することができる（ステップ S354）。なお、ライセンス情報保持部 1440 内に記録された対応するライセンス情報は、ステップ S324 にてアクセス制御情報 AC1 が更新され、再生セッションおよび移動セッションを禁止しているため、消去と同じ状態になっている。なお、この状態にある再生情報に対して、新たなコンテンツデータに対する再生情報の配信あるいは移動を受けた際に、上書きが
- 25 許可されている。

一方、暗号化コンテンツデータ等の保持が指示された場合においては、ステップ S354 はスキップされ、移動処理はこの段階で終了する（ステップ S356）。

暗号化コンテンツデータがメモリ 1415 に記録された状態では、新たに配信

サーバ 30 をアクセスし、再生情報の配信のみを受ければ、再び暗号化コンテンツデータを再生して音楽を聴取することができるようになる。再生情報のみの配信処理は、図 8 および図 9 のフローチャートには図示されていないが、コンテンツデータの授受に関するステップ S 152、S 154、S 156 および S 158
5 を行なわない処理であり、その他については、すでに説明した配信動作と同様であるので説明は繰り返さない。

正常に移動セッションが行なわれた場合の移動処理終了（ステップ S 356）もしくは認証および禁止クラスリストのチェック等によって移動セッションが中止された場合にはステップ S 308、S 310 および S 322 からスキップされて移動セッション全体の処理が終了する（S 360）。
10

このような構成とすることにより、移動セッションにおいても、受信側の携帯電話機に装着されたメモリカードが正規のメモリカードであるか否か、およびクラス証明書が禁止クラスリストの対象であるか否かを事前にチェックした後に、ライセンスキーやコンテンツデータの移動を実行する構成とするので、クラス固有の鍵が破られた再生回路（携帯電話機）もしくはメモリカードに対するコンテンツデータの移動の禁止を行なうことができる。
15

なお、実施の形態 1 においては、禁止クラスリストを運用することによって、データの配信、再生および移動を携帯電話機およびメモリカードのクラスごとに禁止することが可能な構成について説明したが、禁止クラスリストに代えて、許可クラスリスト CPL（Class Permission List）を運用することによって、許可クラスリストにリストアップされたクラスのメモリカードおよび携帯電話機に対してこれらのセッションを有効とする構成も可能である。
20

この場合には、ライセンスサーバ 10 においては、CRL データベース 306 に相当する部分で許可クラスリスト CPL を保持し、メモリカード 110 においては、CRL 保持部 1430 に相当する部分で許可クラスリスト CPL を格納すればよい。
25

さらに、許可クラスリスト CPL による運用を行なう場合には、配信セッションにおけるステップ S 112（図 8）、再生セッションにおけるステップ S 208（図 10）および移動セッションにおけるステップ S 310（図 11）におけ

る含む／含まないの判定を逆にする動作フローを採用すればよい。また、許可クラスリストの運用についても、メモ리카ード内の CPL データの更新は、コンテンツデータ配信時あるいはユーザの要求によって、配信サーバ 30 によって出力される、禁止クラスリストの運用におけるバージョンデータ CRL_ver および差分データ CRL_dat に相当する許可クラスリストの差分データおよびバージョンの更新情報に基づいてメモ리카ード内の CPL リストを書換える構成とすればよい。

この場合においては、クラス固有の鍵が破られた再生回路もしくはメモ리카ードに対応するクラスを逐次許可クラスリスト CPL から削除していく構成とすればよい。このような構成とすることによっても、再生回路およびメモ리카ードのクラスごとに配信、移動および再生セッションの実行を禁止することが可能となる。

また、ステップ S 3 2 4 において、移動を目的としてライセンス情報保持部 1 4 4 0 内の再生情報を取得すると、アクセス制御情報 AC1 を更新し、以降の再生および移動の禁止を記録すると説明したが、当該のデータをライセンス情報保持部 1 4 4 0 から消去することとしても、同様の効果が得られる。

(実施の形態 2)

実施の形態 2 のデータ配信システムにおいては、実施の形態 1 のデータ配信システムの構成と異なって、再生回路共通の秘密鍵 Kcom によって復号可能な暗号化を行なわない点を特徴とする。

すなわち、実施の形態 2 のデータ配信システムは、実施の形態 1 のデータ配信システムが具備する配信サーバ 30 内のライセンスサーバ 10 に代えてライセンスサーバ 11 を備える点で異なる。また、実施の形態 2 のデータ配信システムにおける携帯電話機の構成は、図 6 で説明した携帯電話機 100 の構成に代えて携帯電話機 101 の構成が採用される。

図 13 を参照して、ライセンスサーバ 11 は、ライセンスサーバ 10 と比較して、再生回路共通の秘密鍵 Kcom 保持部 3 2 2 と、秘密鍵 Kcom による暗号化処理部 3 2 4 を具備しない点で異なる。すなわち、ライセンスサーバ 11 においては、配信制御部 3 1 5 が出力するライセンスキー Kc および再生回路制御情報 AC

2は、直接、暗号化処理部326に伝達される。その他の回路構成および動作については図4に示すライセンスサーバ10と同様であるので説明は繰返さない。

以降、ライセンスサーバ11、認証サーバ12および配信キャリア20を合わせて配信サーバ31と総称することとする。

- 5 図14を参照して、携帯電話機101は、実施の形態1で説明した携帯電話機100の構成と比較して、再生回路共通の秘密鍵Kcomを保持するKcom保持部1512と秘密鍵Kcomによる復号処理部1514を具備しない点で異なる。

すなわち、携帯電話機101においては、配信サーバ31において秘密鍵Kcomによる暗号化処理が施されていないことに対応して、セッションキーKs4
10 による復号処理を実行する復号処理部1510によって直接ライセンスキーKcが得られるため、これを復号処理部1510に直接与える構成となる。その他の回路構成および動作については携帯電話機100の場合と同様であるので説明は繰返さない。

また、実施の形態2に従うデータ配信システムにおいて使用されるメモリカード
15 については、図7に示すメモリカード110と同一の構成であるので説明は繰返さない。

次に、再生回路共通の秘密鍵Kcomによる暗号化を省略することによる、配信、再生および移動の各セッションにおける動作の差異についてフローチャートで説明する。

- 20 図15には、実施の形態2に従うデータ配信システムにおける配信動作を説明するためのフローチャートが示される。図15においては、図8および図9で示した実施の形態1に従うデータ配信システムにおける配信動作のフローチャートと異なる点について説明する。

図15を参照して、ステップS132までの処理は、図8で説明したフローチャートと同一である。図13で説明したように、ステップS132で得られるライセンスキーKcおよび再生回路制御情報AC2は、秘密鍵Kcomによる暗号化を
25 施されることなくメモリカード110固有の公開暗号鍵KPm(1)によって暗号化されるので、ステップS134は省略される。以下、ステップS132に続いて、ステップS136～S146に代えて、ステップS136a～S146a

が実行される。

ステップ S 1 3 6 a ~ S 1 4 6 a のそれぞれにおいては、ステップ S 1 3 6 ~ S 1 4 6 において取り扱われるライセンスキー Kc および再生制御情報 AC 2 が、暗号化した形 {Kc//AC 2} Kcom から、そのままの形である Kc//AC 2 に代えられて取扱われる点異なる。その他の暗号化および復号処理については既に図 9 で説明したのと同様であるので説明は繰返さない。

図 1 6 を参照して、実施の形態 2 に従うデータ配信システムにおける再生動作においては、図 1 0 に示した実施の形態 1 に従うデータ配信システムにおける再生動作と比較して、ステップ S 2 2 2 ~ S 2 2 6 に代えて、ステップ S 2 2 2 a ~ S 2 2 6 a が実行される点で異なる。

ステップ S 2 2 2 a ~ S 2 2 6 a のそれぞれにおいては、ステップ S 2 2 2 ~ S 2 2 6 において取り扱われるライセンスキー Kc および再生制御情報 AC 2 が、暗号化した形 {Kc//AC 2} Kcom から、そのままの形である Kc//AC 2 に代えられて取扱われる点異なる。その他の暗号化および復号処理については既に図 1 0 で説明したのと同様であるので説明は繰返さない。また、その他のステップについては図 1 0 と同様であるので説明は繰返さない。

図 1 7 および図 1 8 を参照して、実施の形態 2 に従うデータ配信システムにおける移動セッションにおいては、図 1 1 および図 1 2 に示すステップ S 3 2 6 ~ S 3 3 6 に代えて、ステップ S 3 2 6 a ~ S 3 3 6 a が実行される点で異なる。

ステップ S 3 2 6 a ~ S 3 3 6 a のそれぞれにおいては、ステップ S 3 2 6 ~ S 3 3 6 において取り扱われるライセンスキー Kc および再生回路制御情報 AC 2 が、暗号化した形 {Kc//AC 2} Kcom から、そのままの形である Kc//AC 2 に代えられて取扱われる点異なる。その他の暗号化および復号処理については既に図 1 1 および図 1 2 で説明したのと同様であるので説明は繰返さない。その他のステップについては図 1 1 および図 1 2 と同様であるので説明は繰返さない。

このような構成とすることによって、再生回路に共通な秘密鍵 Kcom を用いない構成としても、実施の形態 1 に従うデータ配信システムと同様の効果を楽しむデータ配信システムを構築することが可能である。

(実施の形態 3)

実施の形態 1 に従うメモリカードにおいては、禁止クラスリスト CRL のデータを TRM 領域内に独自の領域 (図 7 における CRL 保持部 1 4 3 0) を設ける構成としていた。実施の形態 3 に従うメモリカードは、この禁止クラスリスト
5 CRL のデータについてもメモリカード固有の暗号鍵による暗号化を施した上で、TRM 領域外のメモリに暗号化されたコンテンツデータと同様に格納することを特徴とする。

実施の形態 3 におけるメモリカードをメモリカード 1 1 5 とし、メモリカードを識別するための自然数 i および m を、それぞれ $i = 1$ および $m = 1$ として説明
10 する。

図 1 9 を参照して、メモリカード 1 1 5 は、図 7 に示す実施の形態 1 に従うメモリカード 1 1 0 と比較して、TRM 領域内に CRL 保持部 1 4 3 0 を具備しない点で異なる。また、メモリカード 1 1 5 は、TRM 領域内に、共通鍵方式における共通鍵であり、メモリカード 1 1 5 外から参照することのできないメモリカード
15 ごとに固有の共通鍵 $K(1)$ を保持する $K(1)$ 保持部 1 4 5 0 と、共通鍵 $K(1)$ による暗号化処理部 1 4 5 2 および復号処理部 1 4 5 4 をさらに備える。

図 2 0 を参照して、実施の形態 3 に従う配信システムにおいては、図 4 に示した鍵データ等に加えて、メモリカードごとに固有の共通鍵 $K(i)$ が用いられる。共通鍵 $K(i)$ は、メモリカード内のみで扱われる秘密鍵であり、高速に復号可能な対称鍵である点が、同様にメモリカードごとに固有の非対称な一対の鍵である公開暗号鍵 $KPm(i)$ と秘密復号鍵 $Km(i)$ とは異なる。
20

再び図 1 9 を参照して、メモリカード 1 1 5 においては、禁止クラスリスト CRL は、共通鍵 $K(1)$ で暗号化されメモリ 2 4 1 5 に格納される。このように、共通鍵 $K(1)$ で暗号化することで禁止クラスリスト CRL を TRM 領域外に
25 設けられたメモリ 2 4 1 5 に記録することが可能となる。

また、メモリカード 1 1 0 においては、公開暗号鍵 $KPm(1)$ によって暗号化されていたライセンスキー Kc を含む再生情報についても、この共通鍵 $K(1)$ によって暗号化し直すことによって、再生セッションにおける再生開始に至る処理時間の短縮を図ることができる。これは、共通鍵方式における復号が、

公開暗号化方式による復号に対して高速に行なえるためである。また、このような鍵の掛け替えによって、セキュリティ強度が向上する利点も生ずる。

次に、メモリカード 115 を用いたデータ配信システムにおける配信、再生および移動セッションの動作をフローチャートを用いて説明する。

- 5 図 21 および図 22 には、実施の形態 3 に従うデータ配信システムにおける配信動作を説明フローチャートが示される。実施の形態 3 に従うデータ配信システムにおける配信セッション時の動作は、コンテンツ配信リクエストの発生から配信サーバ 30 におけるライセンスキー Kc のデータベースからの取得（ステップ S100）からステップ S142 までについては、図 8 および図 9 に示す場合と同様であるので説明は省略する。

図 22 を参照して、ステップ S142 において、配信サーバ 30 から送信される、暗号化されたライセンスキーを含む再生情報 { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km (1) と禁止クラスリスト CRL の更新に用いられる差分データ CRL_dat とが受理される。

- 15 配信セッション時のメモリカード 115 においては、図 9 に示すステップ S144 および S146 に代えて、ステップ S145 および S147 が実行される。

まず、メモリカード 115 においては、暗号化されたライセンスキーを含む再生情報を Km (1) によって復号し、{Kc//AC2} Kcom、ライセンス ID、コンテンツ ID および AC1 が受理される（ステップ S145）。

- 20 さらに、これらの一部、TRM 領域であるライセンス情報保持部 1440 に記録されない再生情報である {Kc//AC2} Kcom は、共通鍵 K (1) によって暗号化処理部 1452 にて暗号化され、TRM 領域外のメモリ 2415 に記録される（ステップ S147）。

- ステップ S148 においては、実施の形態 1 の場合と同様に、禁止クラスリストのバージョン更新用情報 CRL_dat に基づいてカード内の禁止クラスリスト CRL が更新される。

更新された禁止クラスリストデータ CRL は、同様に暗号化処理部 1452 で K (1) によって暗号化され、暗号化された禁止クラスリスト {CRL} K (1) が TRM 領域外のメモリ 2415 に格納される（ステップ S149）。

その後ステップS 1 5 0から配信処理の終了を示すステップS 1 6 4までは図9で説明したのと同様であるので説明は繰返さない。

図23を参照して、再生リクエストが発生するステップS 2 0 0からコンテンツ再生回路（携帯電話機）の認証を行なうステップS 2 0 6までは図10の場合と同様であるので説明を繰返さない。

メモ리카ード1 1 5においては、禁止クラスリスト CRL を暗号化しメモリ2 4 1 5内に格納しているので、禁止クラスリストのチェックに際して、暗号化された禁止クラスリストデータを復号し取出す処置が必要となる。

メモ리카ード1 1 5においては、認証データ {K_{Pp}(1) // C_p(1)} が認証処理によって正当であると確認され、クラス証明書 C_p(1) が承認された場合には（ステップS 2 0 6）、メモリに記録された {CRL} K(1) を、復号処理部1 4 5 4によって復号して禁止クラスリスト CRL が取得される（ステップS 2 0 7）。コントローラ1 4 2 0は、取得された禁止クラスリスト CRL に応じて、コンテンツ再生回路のクラス証明書 C_p(1) が禁止クラスリストに含まれているかどうかの判定を行なう（ステップS 2 0 8）。

以下、携帯電話機1 1 0が禁止クラスリスト CRL の対象外であり、正常に再生が実行される場合には、ステップS 2 1 0からステップS 2 2 0までが図10に説明したのと同様に実行される。

メモ리카ード1 1 5においては、図10で説明したメモ리카ード1 1 0におけるステップS 2 2 2に代えて、ステップS 2 2 2 bが実行される。ステップS 2 2 2 bにおいては、メモリに記録された、ライセンスキーK_c および再生制御情報 AC2 が共通鍵 K(1) によって暗号化された { {K_c//AC2} K_{com}} K(1) としてメモリ2 4 1 5に記録されているため、この暗号化データを復号処理部1 4 5 4において共通鍵 K(1) によって復号し {K_c//AC2} K_{com} を取得するものである。

その後のステップS 2 2 4～ステップS 2 4 0についても図10の場合と同様であるので説明は繰返さない。

図24および図25には、メモ리카ード1 1 5を備えたデータ配信システムにおける移動セッションの動作を説明するフローチャートが示される。

図 2 4 および図 2 5 においては、送信側を携帯電話機 1 0 0 およびメモ리카ード 1 1 5 とし、受信側を携帯電話機 1 0 2 およびメモ리카ード 1 1 6 とする。図 1 1 および図 1 2 の場合と同様に、メモ리카ード 1 1 6 に対応する自然数 $i=2$, $m=2$ とする。

5 図 2 4 のフローチャートを、実施の形態 1 で説明した図 1 1 のフローチャートと比較すると、メモ리카ード 1 1 5 においては、再生セッションの場合と同様に、メモ리카ードの $KP_{mc}(2)$ の認証を実行するステップ S 3 0 8 において、認証が有効であった場合には、引続き禁止クラスリストの対象であるか否かを判定する場合に、メモリ 2 4 1 5 内に格納された禁止クラスリストの暗号化データ {CRL} K (1) を復号する必要があるが生じる。

10 具体的には、ステップ S 3 0 8 の認証結果が有効であれば、コントローラ 1 4 2 0 は、メモリ 2 4 1 5 から暗号化された禁止クラスリスト {CRL} K (1) を読出して、復号処理部 1 4 5 4 で復号処理し禁止クラスリスト CRL を取得する (ステップ S 3 0 9)。

15 取得した禁止クラスリスト CRL に基づいて、ステップ S 3 1 0 においてメモ리카ードのクラス証明書が禁止クラスリストの対象となっていないかどうか判定される。図 2 4 および図 2 5 に示される、ステップ S 3 1 0 以降の処置については図 1 1 および図 1 2 に示したのと同様であるので説明を繰返さない。

20 このような構成とすることにより、禁止クラスリスト CRL のデータ格納する部分を TRM 内に特別に設ける必要はなくなるので、実施の形態 1 に従うメモ리카ードを用いるデータ配信システムが奏する効果に加えて、メモ리카ードの製造コストが低減されるという利点がある。

25 また、メモリ 2 4 1 5 に格納される禁止クラスリストデータ CRL、ライセンスキー K_c および再生制御情報 AC2 は、対象鍵である共通鍵 K (1) によって新たに暗号化されるので、メモ리카ードのセキュリティ強度が向上するとともに、データの復号処理を高速に実行できるという利点もさらに生じる。

なお、禁止クラスリストデータ CRL を、TRM 領域外のメモリ領域 2 4 1 5 内に設けることだけを目的とすれば、共通鍵 K (1) を用いずに、メモ리카ード固有の公開暗号鍵 $KP_m(1)$ で禁止クラスリスト CRL を暗号化しメモリ 2 4 1 5

内に {CRL} Km (1) として格納することによっても実現することが可能である。

すべての実施の形態に従うデータ配信システムにおける配信動作における配信サーバ10の認証処理において、配信サーバ10は、メモリカード110および携帯電話機（コンテンツ再生回路）100の認証データ {KPmc (1) //Cmc (1) } KPma および {KPp (1) //Cp (1) } KPma をともに認証するように説明したが、メモリカードは着脱可能であることから、音楽を再生するコンテンツ再生回路が、必ずしも配信を受けた携帯電話機と同一である必然性はない。また、再生に際してメモリカード内においても再生情報の一部（ライセンスキーKc および再生回路制限情報 AC2）を出力するにあたって、出力先のコンテンツ再生回路の認証データ {KPp (1) //Cp (1) } KPma の認証処理を行っており、配信サーバにおけるコンテンツ再生回路の認証データ {KPp (1) //Cp (1) } KPma の認証処理を行わなくても、セキュリティの低下につながらない。

これらの理由から、配信サーバにおけるコンテンツ再生回路の認証データ {KPp (1) //Cp (1) } KPma の認証処理を行わず、直接の配信先にあたるメモリカード110の認証データ {KPmc (1) //Cmc (1) } KPma の認証処理のみを行なう構成とすることもできる。

この場合、実施の形態1および2に対する図8と、実施の形態に対応する図21において、ステップS104、S106、S108、S110およびS112において、携帯電話機（コンテンツ再生回路）100の認証データ {KPp (1) } KPma、公開暗号鍵 KPp (1) クラス証明書 Cp (1) に対する処理をすべて省略すれば実現することができる。

また、ステップS104において、コンテンツID、メモリカード110の認証データ {KPmc (1) //Cmc (1) } KPma およびライセンス購入条件 AC を配信サーバに送信し、ステップS106において、配信サーバ10はメモリカード110の認証データ {KPmc (1) //Cmc (1) } KPma およびライセンス購入条件 AC を受信し、ステップS108において、認証鍵 KPma によって、認証データ {KPmc (1) //Cmc (1) } KPma を復号し、さらに、ステップS110において、復号結果に基づいて認証処理を行ない、正当なメモリカードからの認証デ

ータである場合においては、クラス証明書 Cmc (1) を承認する。一方、認証データが正当でない場合においては、配信処理は終了する。

5 ステップ S 1 1 2 において、承認したクラス証明書 Cmc (1) が CRL データベース 3 0 6 からの禁止クラスリスト CRL にリストアップされたクラス証明書に含まれるかどうかを判断する。禁止クラスリスト CRL に含まれなければ配信処理は続けられ、含まれた場合には配信処理は終了する。以降のステップにおける処理については、このような認証処理を行なった場合においても、実施の形態 1 および 2 で説明したのと同様に実行することができる。

10 また、再生動作および移動動作においては、このような認証処理を行なうこととしても、実施の形態 1 および 2 ですでに説明したのと同様のフローに従って処理することができる。

さらに、実施の形態 1 および 2 に用いたメモ리카ード 1 1 0 において、十分な TRM 領域が確保できる場合において、ライセンス保持部 1 4 4 0 に、復号して平文となったすべての再生情報 (ライセンスキー Kc、再生回路制御情報 AC 2、
15 ライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1) を保持しても、セキュリティ上の問題はなく、メモ리카ード 1 1 0 の処理が変更になるのみで、同様な効果を得ることができる。

以下に、平文となったすべての再生情報をライセンス保持部 1 4 4 0 に保持するケースに対応するために、実施の形態 1 および 2 で説明した、配信処理、再生
20 処理および移動処理の動作フローに変更を加える必要がある個所について説明する。

このようなケースに対応するためには、実施の形態 1 に従う配信処理においては、図 9 におけるステップ S 1 4 4 を省いて、ステップ S 1 4 6 において、復号して得られたすべての再生情報 (ライセンスキー Kc、再生回路制御情報 AC 2、
25 ライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1) を受理し、ステップ S 1 5 0 において、受理したすべての再生情報をライセンス情報保持部 1 4 4 0 に記録すればよい。

実施の形態 1 に従う再生処理においては、図 1 0 におけるステップ S 2 2 0 において、ライセンス情報保持部に記録されている再生リクエスト曲の {Kc//AC

2) Kcom を取得するように変更する。再生処理における他のステップにおいては処理の変更は必要ない。

5 実施の形態 1 に従う移動処理においては、図 1 1 におけるステップ S 3 2 4 において、ライセンス情報保持部 1 4 4 0 に保持されたすべての再生情報を取得して、ステップ S 3 2 6 の処理を省略すればよい。その他のステップに対する変更は必要ない。

10 同様に、実施の形態 2 に従う配信処理においては、図 1 5 中のステップ S 1 4 4 a を省略して、ステップ S 1 4 6 a において、復号して得られたすべての再生情報（ライセンスキー Kc、再生回路制御情報 AC 2、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1）を受理し、ステップ S 1 5 0 において、受理したすべての再生情報をライセンス情報保持部 1 4 4 0 に記録すればよい。

15 また、実施の形態 2 に従う再生処理においては、図 1 6 中のステップ S 2 2 2 a における処理を、ライセンス情報保持部 1 4 4 0 に記録されている再生リクエスト曲のライセンスキー Kc および再生回路制限情報 AC 2 を取得するように変更するのみでよく、他のステップにおける動作の変更は必要ない。

実施の形態 2 に従う移動処理においては、図 1 7 中のステップ S 3 2 4 において、ライセンス情報保持部 1 4 4 0 に保持されたすべての再生情報を取得して、ステップ S 3 2 6 a の処理を省略することによって対応できる。

20 以上に説明した動作フローの変更を行うことによって、平文となったすべての再生情報をライセンス保持部 1 4 4 0 に保持するケースにおいても、実施の形態 1 および 2 と同様の、配信処理、再生処理および移動処理を実行することができる。

25 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内のすべての変更が含まれることが意図される。

産業上の利用可能性

30 この発明によるデータ配信システムおよび記録装置は、携帯電話機のような移動通信端末を利用したデータ配信に用いることができる。

請求の範囲

1. データ配信システムであって、
複数の端末（100, 101）と、
5 暗号化コンテンツデータ（{Data} Kc）と、前記暗号化コンテンツデータを
復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンス
キー（Kc）とを前記複数の端末に配信するためのコンテンツ供給装置（10,
11）とを備え、
各前記端末は、
10 外部との間でデータを授受するための第1のインタフェース部（1102）と、
少なくとも前記ライセンスキーを受けて記録する配信データ解読部（110,
115）とを含み、
前記配信データ解読部は、
15 認証鍵（KPma）によって復号することで認証可能な状態に暗号化された、前
記配信データ解読部に対応して定められる第1のクラス証明データ（Cmc(m）
を保持し、前記ライセンスキーを受信する場合に、前記第1のインタフェース部
を介して出力する第1の認証データ保持部（1400）と、
前記暗号化コンテンツデータおよび前記ライセンスキーを記録するための第1
の記憶部（1415, 1440）とを有し、
20 前記コンテンツ供給装置は、
外部との間でデータを授受するための第2のインタフェース部（350）と、
前記認証鍵によって復号することで正当性を証明できる状態に暗号化された前
記第1のクラス証明データを前記第2のインタフェース部から受け取って、前記
認証鍵によって復号して前記正当性を確認するための第1の認証処理部（31
25 2）と、
前記配信の禁止対象となされる前記第1のクラス証明データをリストアップし
た禁止クラスリスト（CRL）を保持するための禁止クラスリスト保持部（30
6）と、
前記第1の認証処理部において得られた前記第1のクラス証明データが禁止ク

ラスリスト保持部に保持される前記禁止クラスリストに含まれる場合には、前記少なくとも前記コンテンツキーの配信動作を中止する配信制御部（315）とを含む、データ配信システム。

2. 前記配信データ解読部（110, 115）は、前記端末に着脱可能な記録装置であり、

前記第1のクラス証明データ（Cmc(m)）は、前記記録装置の種類ごとに対応して予め定められる、請求の範囲第1項に記載のデータ配信システム。

3. 前記配信データ解読部（110, 115）は、

前記禁止クラスリスト（CRL）を保持するための第2の記憶部（1430, 2145）と、

前記配信動作が指示されるのに応じて、前記第2の記憶部に保持される前記禁止クラスリストの更新を特定できる更新情報（CRL_ver）を抽出して、前記第2のインタフェース部（1102）を介して前記コンテンツ供給装置（10, 11）に対して出力する制御部（1420）とをさらに有し、

前記コンテンツ供給装置は、前記更新情報を前記第2のインタフェース部（350）を介して前記配信制御部（315）へ与え、

前記配信制御部は、前記更新情報に基づいて、前記第2の記憶部に保持される前記禁止クラスリストを新しい禁止クラスリストに更新するための更新データ（CRL_dat）を作成し、前記第2のインタフェース部を介して前記更新データを出力し、

前記制御部は、前記第1のインタフェース部を介して受けた前記更新データに基づいて、前記第2の記憶部に保持される前記禁止クラスリストの内容を更新する、請求の範囲第1項に記載のデータ配信システム。

4. 前記配信データ解読部（110, 115）は、

前記認証鍵（KPma）による復号を行なって前記正当性を確認するための第2の認証処理部（1408）をさらに有し、

前記配信データ解読部は、外部から指示される、前記暗号化コンテンツデータ（{Data} Kc）および前記ライセンスキー（Kc）の少なくとも一方を他の配信データ解読部（112, 116）に移動させる移動動作において、前記他の配信

データ解読部に対応する、前記認証鍵によって復号することで前記正当性が証明できる状態に暗号化された、前記第1のクラス証明データ (Cmc(m)) を取得し、

前記制御部 (1420) は、前記第2の認証処理部において得られた前記他の配信データ解読部に対応する前記第1のクラス証明データが前記第2の記憶部 (1430, 2145) に保持される前記禁止クラスリスト (CRL) に含まれる場合には、少なくとも前記ライセンスキーの前記移動動作を中止する、請求の範囲第3項に記載のデータ配信システム。

5 5. 各前記端末 (100, 101) は、コンテンツ再生部 (1550) をさらに含み、

10 前記コンテンツ再生部は、

前記配信データ解読部 (110, 115) から前記ライセンスキー (Kc) と前記暗号化コンテンツデータ (Data) Kc) とを受けて、前記ライセンスキーにより前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部 (1516, 1518) と、

15 前記認証鍵 (KPma) によって復号することで前記正当性が証明できる状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第2のクラス証明データ (Cp(n)) を保持する第2の認証データ保持部 (1500) とを有し、

前記第1の認証処理部 (312) は、暗号化された前記第2のクラス証明データを、前記第2のインタフェース部 (350) から受け取って復号処理を行ない、

20 前記禁止クラスリスト保持部 (306) に保持された前記禁止クラスリスト (CRL) は、禁止対象とされる前記第2のクラス証明データをさらにリストアップし、

前記配信動作において、各前記端末 (100, 101) は、暗号化された前記第2のクラス証明データを前記第1のインタフェース部 (1102) を介して前記第2のインタフェース部に対して出力し、

25 前記配信制御部 (315) は、前記第2のインタフェース部を介して入力され、前記第1の認証処理部によって復号された前記第2のクラス証明書データが、前記禁止クラスリスト保持部に保持される前記禁止クラスリストに含まれる場合には、前記配信動作を中止する、請求の範囲第1項に記載のデータ配信システム。

6. 各前記端末は、コンテンツ再生部（1550）をさらに備え、

前記コンテンツ再生部は、

前記配信データ解読部（110, 115）から前記ライセンスキー（Kc）と
前記暗号化コンテンツデータ（{Data} Kc）とを受けて、前記ライセンスキー
5 により前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部
（1516, 1518）と、

前記認証鍵（KPma）によって復号することで前記正当性が証明可能な状態に
暗号化された、前記コンテンツ再生部に対応して予め定められる第2のクラス証
明データ（Cp(n)）を保持する第2の認証データ保持部（1500）とを有し、

10 前記配信データ解読部は、

前記認証鍵による復号を行って前記正当性を確認するための第2の認証処理部
（1408）をさらに有し、

前記第2の記憶部（1430, 2145）に保持された前記禁止クラスリスト
（CRL）は、禁止対象となされる前記第2のクラス証明データをさらにリストア
15 ップし、

前記配信データ解読部は、外部から指示される、前記暗号化コンテンツデータ
を前記コンテンツ再生部によって再生する再生動作において、前記第1の記憶部
（1415, 1440）から前記暗号化コンテンツデータおよびライセンスキー
を出力し、

20 前記配信データ解読部は、前記再生動作において、前記コンテンツ再生部に対
応する、前記認証鍵によって復号することで前記正当性が証明できる状態に暗号
化された前記第2のクラス証明データを取得し、

前記制御部（1420）は、前記再生動作時において、前記第2の認証処理部
によって得られた前記第2のクラス証明データが前記第2の記憶部に保持される
25 前記禁止クラスリストに含まれる場合には、前記再生動作を中止する、請求の範
囲第3項に記載のデータ配信システム。

7. 前記第1のインタフェース部（350）と前記第2のインタフェース部
（1102）とは、携帯電話網によって接続され、

前記配信制御部（315）は、前記配信動作時において、前記第1のクラス証

明データ (Cmc(m)) に基づいて前記配信データ解読部 (110, 115) の認証を行なう、請求の範囲第1項に記載のデータ配信システム。

8. 各前記端末 (100, 101) は、前記携帯電話網に接続して通話を行なう通信処理部をさらに含む、請求の範囲第7項に記載のデータ配信システム。

5 9. 前記コンテンツ再生部 (1550) は、前記端末 (100, 101) に着脱可能な構成である、請求の範囲第5項に記載のデータ配信システム。

10. 前記第1の記憶部 (1415, 1440) は、半導体メモリであり、前記記録装置は、メモリカードである、請求の範囲第2項に記載のデータ配信システム。

10 11. 記録装置であつて、

データを (Kc) を記録するための第1の記憶部 (1415, 1440) と、
インタフェース部 (1202) を介して入力される、認証鍵 (KPma) によって復号することで認証可能な状態に暗号化された第1のクラス証明データ (Cp(n)) を受けて、前記認証鍵 (KPma) による復号を行なって正当性を確認するための認証処理部 (1408) と、

15 前記データの出力を禁止する対象となされる第1のクラス証明データをリストアップした禁止クラスリスト (CRL) を保持するための第2の記憶部 (1430, 2145) と、

20 外部からの前記データの出力指示に応じて、前記インタフェース部を介して前記データの出力を指示する制御部 (1420) とを備え、

前記制御部は、前記出力指示とともに外部から前記インタフェース部を介して入力される、前記暗号化がなされた第1のクラス証明データを前記認証処理部で復号して得られる前記第1のクラス証明データが前記禁止クラスリストに含まれる場合において、前記データの出力を中止する、記録装置。

25 12. 前記認証鍵 (KPma) によって復号可能な状態に暗号化された、前記記録装置に対応して定められる第2のクラス証明データ (Cmc(m)) を保持する認証データ保持部 (1400) をさらに備え、

前記認証データ保持部は、外部からの前記データ (Kc) の入力指示に応じて、前記認証データ保持部に保持される、前記認証鍵によって復号することで正当性

を証明できる状態に暗号化された前記第2のクラス証明データを前記インタフェース部(1202)を介して出力する、請求の範囲第11項に記載の記録装置。

13. 前記入力指示に応じて、前記インタフェース部(1202)を介して前記データ(Kc)の入力を受けて、前記第1の記憶部(1415, 1440)に記録する記録動作において、

前記制御部(1420)は、前記記録動作が指示されるのに応じて、前記第2の記憶部(1430, 2145)に保持される前記禁止クラスリスト(CRL)の更新を特定できる更新情報(CRL_ver)を抽出し、前記更新情報を前記インタフェース部を介して外部に出力し、

前記制御部は、前記更新情報に基づいて生成される、前記禁止クラスリストを新しい禁止クラスリストに更新するための更新データ(CRL_dat)を、外部から前記インタフェース部を介して受けて、前記更新データに基づいて前記禁止クラスリストの内容を更新する、請求の範囲第12項に記載の記録装置。

14. 前記第1の記憶部(1415, 1440)は、半導体メモリであり、

前記記録装置は、メモリカードである、請求の範囲第11項に記載の記録装置。

15. データ配信システムであって、

暗号化コンテンツデータ({Data} Kc)と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ(Data)を得るための復号鍵であるライセンスキー(Kc)とを配信するためのコンテンツ供給装置(10, 11)と、

前記コンテンツ供給装置(10, 11)からの前記配信を受ける複数の端末(100, 101)とを備え、

前記コンテンツ供給装置は、

外部との間でデータを授受するための第1のインタフェース部(350)と、

認証鍵(KPma)によって復号することで認証可能な状態に暗号化された、第1のクラス証明データ(Cmc(m))および第1の公開暗号鍵(KPmc(m))を、前記第1のインタフェース部から受けて前記認証鍵による復号を行なって正当性を確認するための第1の認証処理部(312)と、

前記ライセンスキーの配信の禁止対象となされる前記第1のクラス証明データをリストアップした禁止クラスリスト(CRL)を保持する禁止クラスリスト保持

部（３５０）と、

前記第１の認証処理部において得られた前記第１のクラス証明データが前記禁止クラスリスト保持部に保持される前記禁止クラスリストに含まれる場合には、
少なくとも前記ライセンスキーを含む第１の再生情報の配信動作を中止する配信
5 制御部（３１５）と、

前記配信ごとに更新される第１の共通鍵（ $Ks1$ ）を生成する第１のセッション
キー発生部（３１６）と、

前記第１の公開暗号鍵によって前記第１の共通鍵を暗号化して前記第１のイン
タフェース部に与えるためのセッションキー暗号化部（３１８）と、

10 前記第１の共通鍵によって暗号化されて前記第１のインタフェース部を介して
返信される、第２の公開暗号鍵（ $KPm(i)$ ）および第２の共通鍵（ $Ks2$ ）を復号抽
出するためのセッションキー復号部（３２０）と、

前記第１の再生情報を、前記セッションキー復号部により復号された前記第２
の公開暗号鍵によって暗号化する第１のライセンスデータ暗号化処理部（３２
15 ６）と、

前記第１のライセンスデータ暗号化処理部の出力を、前記セッションキー復号
部により復号された前記第２の共通鍵によってさらに暗号化して、前記第１の
インタフェース部に与え配信するための第２のライセンスデータ暗号化処理部
（３２８）とを含み、

20 各前記端末は、

外部との間でデータを授受するための第２のインタフェース部（１１０２）と、
前記暗号化コンテンツデータを受けて記録する配信データ解読部（１１０、１
1 ５）とを含み、

25 第１のクラス証明データ（ $Cmc(m)$ ）および第１の公開暗号鍵（ $KPmc(m)$ ）は、
前記配信データ解読部に対応して定められ、

前記配信データ解読部は、

前記認証鍵によって復号することで前記正当性を証明できる状態に暗号化され
た、前記第１のクラス証明データおよび前記第１の公開暗号鍵を保持し、前記第
１の再生情報を受信する場合に出力する第１の認証データ保持部（１４００）と、

前記第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵 ($K_{mc}(m)$) を保持する第1の鍵保持部 (1402) と、

前記第1の公開暗号鍵によって暗号化された前記第1の共通鍵を受けて、復号処理するための第1の復号処理部 (1404) と、

5 前記第2の公開暗号鍵を保持する第2の鍵保持部 (1416) と、

前記暗号化コンテンツデータの通信ごとに更新される前記第2の共通鍵を生成する第2のセッションキー発生部 (1418) と、

前記第2の共通鍵および前記第2の公開暗号鍵を前記第1の共通鍵によって暗号化し、前記第2のインタフェース部に出力するための第1の暗号化処理部 (1

10 406) と、

前記第2のライセンスデータ暗号化処理部から、暗号化された前記第1の再生情報を受けて、前記第2の共通鍵によって復号するための第2の復号処理部 (1412) と、

15 前記第2の公開暗号鍵によって暗号化されたデータを復号するための第2の秘密復号鍵 ($K_{m}(i)$) を保持する第3の鍵保持部 (1421) と、

前記第2の秘密復号鍵による復号処理を実行するための第3の復号処理部 (1422) と

前記第1の再生情報および前記暗号化コンテンツデータを記録するための第1の記憶部 (1415, 1440) とを有する、データ配信システム。

20 16. 前記配信データ解読部 (110, 115) は、前記端末 (100, 101) に着脱可能な記録装置であり、

前記第1の秘密復号鍵 ($K_{mc}(m)$) は、前記記録装置の種類ごとに異なる、請求の範囲第15項に記載のデータ配信システム。

25 17. 前記第2および前記第3の復号処理部 (1412, 1422) は、前記コンテンツ供給装置 (10, 11) において前記第2の公開暗号鍵 ($K_{Pm}(i)$) で暗号化され、さらに前記第2の共通鍵 (K_{s2}) で暗号化されて、前記第1の再生情報とともに配信される第2の再生情報 ($AC1$) を前記第2のインタフェース部 (1102) を介して受け、前記第2の共通鍵および前記第2の秘密復号鍵 ($K_{m}(i)$) によって復号し、

前記第1の記憶部(1415, 1440)は、前記第2の再生情報をさらに記録する、請求の範囲第15項に記載のデータ配信システム。

18. 前記配信データ解読部(110, 115)は、

5 前記禁止クラスリスト(CRL)を保持するための第2の記憶部(1430, 2415)と、

前記暗号化コンテンツデータ({Data} Kc)の配信動作が指示されるのに応じて、前記第2の記憶部に保持される前記禁止クラスリストの更新を特定できる更新情報(CRL_ver)を生成する制御部(1420)とをさらに有し、

10 前記第1の暗号化処理部(1406)は、さらに、前記更新情報を前記第1の共通鍵(Ks1)によって暗号化して前記第2のインタフェース部(1102)に出力し、

前記配信制御部(315)は、前記セッションキー復号部(320)によって復号された前記更新情報に基づいて、前記第2の記憶部に保持される前記禁止クラスリストを新しい禁止クラスリストに更新するための更新データ(CRL_dat)を生成し、

15 前記コンテンツ供給装置は、前記更新データを前記第2の共通鍵(Ks2)で暗号化して前記第1のインタフェース部(350)より出力し、

前記第2の復号処理部(1412)は、前記第2のインタフェース部を介して受ける暗号化された前記更新データを前記第2の共通鍵によって復号し、

20 前記制御部(1420)は、前記更新データに基づいて、前記第2の記憶部に保持される前記禁止クラスリストの内容を更新する、請求の範囲第15項に記載のデータ配信システム。

19. 前記第2の記憶部(1430, 2145)は、第三者に読出不可なセキュリティ領域(TRM)内に配置される、請求の範囲第18項に記載のデータ配信システム。

25 20. 前記第2のセッションキー発生部(1418)は、外部から指示される前記コンテンツデータの再生動作においては、前記指示にตอบสนองして第3の共通鍵(Ks3)を生成し、

前記第1の記憶部(1415, 1440)は、前記制御部(1420)に制御

されて、前記再生動作の指示に応じて、記録した前記暗号化コンテンツデータ
({Data} Kc) および前記第 1 の再生情報を出力し、

前記第 3 の復号処理部 (1 4 2 2) は、前記再生動作において、前記第 1 の記憶部から出力された前記第 1 の再生情報が暗号化されている場合に、復号を行な
5 って前記第 1 の再生情報を抽出し、

前記第 1 の暗号化処理部 (1 4 0 6) は、前記再生動作においては、前記第 3 の復号処理部および前記第 1 の記憶部のいずれか一方から前記第 1 の再生情報を受けて、第 4 の共通鍵 (Ks4) に基づいて暗号化し、

前記配信データ解読部 (1 1 0 , 1 1 5) は、前記第 4 の共通鍵によって暗号
10 化された前記第 1 の再生情報および前記暗号化コンテンツデータを出力し、

各前記端末 (1 0 0 , 1 0 1) は、コンテンツ再生部 (1 5 5 0) をさらに含み、

前記コンテンツ再生部は、

前記配信データ解読部からの、前記第 4 の共通鍵によって暗号化された前記第
15 1 の再生情報を復号して、前記第 1 の再生情報を抽出する第 4 の復号処理部 (1 5 1 0) と、

前記暗号化コンテンツデータを、前記第 4 の復号処理部からの出力である前記第 1 の再生情報に含まれる前記ライセンスキー (Kc) により復号して再生する
コンテンツデータ再生部 (1 5 1 6 , 1 5 1 8) と、

20 前記認証鍵 (KPma) によって復号することで正当性を証明できる状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第 2 のクラス証明データ (Cp (n)) および第 3 の公開暗号鍵 (Kpp(n)) を保持し、前記再生動作に応じて前記配信データ解読部 (1 1 0 , 1 1 5) に対して出力する第 2 の認証データ保持部 (1 5 0 0) と、

25 前記第 3 の公開暗号鍵によって暗号化されたデータを復号化するための第 3 の秘密復号鍵 (Kp(n)) を保持する第 4 の鍵保持部 (1 5 0 2) と、

前記第 3 の公開暗号鍵によって暗号化されて返信されるデータを前記第 3 の秘密復号鍵によって復号して前記第 3 の共通鍵を得るための第 5 の復号処理部 (1 5 0 4) と、

前記再生動作ごとに更新される前記第4の共通鍵を生成する第3のセッションキー発生部(1508)と、

前記第5の復号処理部から受ける前記第3の共通鍵によって、前記第4の共通鍵を暗号化して前記配信データ解読部に対して出力する第2の暗号化処理部(1

5 506)とを有し、

前記配信データ解読部(110, 115)は、

前記認証鍵によって復号することで正当性を証明できる状態に暗号化された、前記第2のクラス証明データおよび前記第3の公開暗号鍵を、前記認証鍵(KPma)によって復号して前記正当性を確認するための第2の認証処理部(14

10 08)と、

前記制御部(1420)に制御されて、前記第2の認証処理部から受ける前記第3の公開暗号鍵によって前記第2の共通鍵を暗号化して、対応する前記コンテンツ再生部(1550)に対して出力するための第3の暗号化処理部(1410)とをさらに有し、

15 前記禁止クラスリスト(CRL)は、禁止対象とされる前記第2のクラス証明データをさらにリストアップし、

前記制御部(1420)は、前記再生動作において、前記第2の認証処理部において得られた前記第2のクラス証明データが前記第2の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記再生動作を中止する、請求の

20 範囲第18項に記載のデータ配信システム。

21. 前記第2および前記第3の復号処理部(1412, 1422)は、前記コンテンツ供給装置(10, 11)において前記第2の公開暗号鍵(KPm(i))で暗号化され、さらに前記第2の共通鍵(Ks2)で暗号化されて、前記第1の再生情報(AC2)とともに配信される第2の再生情報(AC1)を前記第2のインタフェース部(1102)を介して受けて、前記第2の共通鍵および前記第2の秘密復号鍵(Km(i))によって復号し、

25

前記第1の記憶部(1440)は、配信データ解読部(110, 115)は、復号された前記第2の再生情報をさらに記録し、

前記制御部(1420)は、前記再生動作において、前記第1の記憶部に記録

された前記第 2 の再生情報に基づいて前記第 1 の再生情報の出力可否を判断する、
請求の範囲第 20 項記載のデータ配信システム。

22. 前記第 2 の認証処理部 (1408) は、外部から指示される、前記配信データ
5 1 1 0, 1 1 5) から他の配信データ解読部 (1 1 2, 1 1 6) に対して少なくとも前記第 1 の再生情報を含むデータを移転するための移動
動作に応じて、前記認証鍵によって復号することで正当性を証明できる状態に暗
号化された、前記他の配信データ解読部に対応する、前記第 1 のクラス証明デー
タ (Cmc(m)) および前記第 1 の公開暗号鍵 (KPmc(m)) を前記第 2 のインタフ
ェース部から受け取って、前記認証鍵(KPma)によって復号して前記正当性を確
10 認し、

前記配信データ解読部および前記他の配信データ解読部にそれぞれ対応する複
数の前記第 2 のセッションキー発生部 (1418) は、前記移動動作に応じて、
前記第 3 および第 2 の共通鍵 (Ks3, Ks2) をそれぞれ生成し、

前記第 3 の暗号化処理部 (1410) は、前記移動動作時において、前記他の
15 配信データ解読部に対応する前記第 1 の公開暗号鍵によって前記配信データ解読
部 (1 1 2, 1 1 6) に対応する前記第 3 の共通鍵を暗号化して、前記他の配信
データ解読部に対して出力し、

前記第 2 の復号処理部 (1412) は、前記移動動作時において、前記第 3 の
共通鍵によって暗号化されて前記他の配信データ解読部から返信されるデータを
20 復号して、前記他の配信データ解読部 (1 1 2, 1 1 6) で生成された前記第 2
の共通鍵および前記他の配信データ解読部に対応する前記第 2 の公開暗号鍵を取
得し、

前記配信データ解読部は、

前記移動動作において、前記第 1 の記憶部 (1440) から出力される前記第
25 1 の再生情報を、前記他の配信データ解読部に対応する前記第 2 の公開暗号鍵に
よってさらに暗号化するための第 4 の暗号化処理部 (1424) と、

前記移動動作時において、前記第 4 の暗号化処理部 (1424) の出力および
前記第 2 の復号処理部 (1412) によって取得された前記第 2 の共通鍵を前記
第 1 の暗号化処理部 (1406) に伝達するためのデータスイッチ (1442,

1 4 4 6) とをさらに有し、

前記第 1 の暗号化処理部 (1 4 0 6) は、前記移動動作時において、前記第 4 の暗号化処理部 (1 4 2 4) の出力を、前記他の配信データ解読部 (1 1 2, 1 1 6) で生成された前記第 2 の共通鍵によってさらに暗号化して、前記他の配信データ解読部に対して出力し、

前記制御部 (1 4 2 0) は、前記移動動作において、前記第 2 の認証処理部において得られた前記他の配信データ解読部に対応する前記第 1 のクラス証明データが前記第 2 の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記移動動作を中止する、請求の範囲第 2 0 項に記載のデータ配信システム。

2 3. 前記制御部 (1 4 2 0) は、前記移動動作において、前記他の配信データ解読部 (1 1 2, 1 1 6) に対応する前記第 1 のクラス証明データ (Cmc(m)) に基づいて、前記他の配信データ解読部の認証を行なう、請求の範囲第 2 2 項に記載のデータ配信システム。

2 4. 前記第 4 の暗号化処理部 (1 4 2 4) は、前記禁止クラスリストのデータを前記第 2 の公開暗号鍵 (KPm(i)) で暗号化し、

前記第 2 の記憶部 (2 4 1 5) は、第三者に読出不可能なセキュリティー領域 (TRM) 外に設けられて、前記第 4 の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第 2 2 項に記載のデータ配信システム。

2 5. 前記第 2 および前記第 3 の復号処理部 (1 4 1 2, 1 4 2 2) は、前記コンテンツ供給装置 (1 0, 1 1) において前記第 2 の公開暗号鍵 (KPm(i)) で暗号化され、さらに前記第 2 の共通鍵 (Ks2) で暗号化されて、前記第 1 の再生情報 (AC2) とともに配信される第 2 の再生情報 (AC1) を前記第 2 のインタフェース部 (1 1 0 2) を介して受け、前記第 2 の共通鍵および前記第 2 の秘密復号鍵 (Km(i)) によって復号し、

前記第 1 の記憶部 (1 4 4 0) は、復号された前記第 2 の再生情報をさらに記録し、

前記制御部 (1 4 2 0) は、前記移動動作時において、前記第 1 の記憶部に記録された第 2 の再生情報に基づいて前記移動動作の実行可否を判断するとともに、前記暗号化コンテンツデータ ({Data} Kc) を前記他の配信データ解読部 (1

1 2, 1 1 6) に出力することを指示した場合には前記第 2 の再生情報を更新する、請求の範囲第 2 0 項に記載のデータ配信システム。

2 6. 前記制御部 (1 4 2 0) は、前記再生動作において、前記第 2 のクラス証明データ (Cp(n)) に基づいて前記コンテンツ再生部 (1 5 5 0) の認証を行なう、請求の範囲第 2 0 項に記載のデータ配信システム。

2 7. 前記配信データ解読部 (1 1 5) は、

前記記録装置ごとに異なる秘密鍵 (K(i)) を保持する第 5 の鍵保持部 (1 4 5 0) と、

前記第 2 の復号処理部 (1 4 1 2) の出力を前記第 3 の復号処理部 (1 4 2 2) において前記第 2 の秘密復号鍵 (Km(i)) によって復号して得られるデータを前記秘密鍵で暗号化するための第 5 の暗号化処理部 (1 4 5 2) と、

前記秘密鍵で暗号化されたデータを復号するための第 6 の復号処理部 (1 4 5 4) とをさらに有し、

前記第 1 の記憶部 (1 4 1 5) は、前記第 5 の暗号化処理部によって暗号化されたデータを記録し、

前記第 5 の暗号化処理部は、前記禁止クラスリスト (CRL) のデータを前記秘密鍵で暗号化し、

前記第 2 の記憶部 (2 4 1 5) は、第三者に読出不可能なセキュリティー領域 (TRM) 外に設けられて、前記第 5 の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第 1 8 項に記載のデータ配信システム。

2 8. 前記コンテンツ供給装置 (1 0, 1 1) は、

前記コンテンツ再生部 (1 5 5 0) にて再生可能な共通秘密鍵 (Kcom) を保持する第 6 の鍵保持部 (3 2 2) と、

前記第 1 の再生情報を前記共通秘密鍵によって暗号化し、前記第 1 のライセンスデータ暗号化処理部 (3 2 6) に対して出力する第 3 のライセンスデータ暗号化部 (3 2 4) をさらに含み、

前記コンテンツ再生部 (1 5 5 0) は、

前記共通秘密鍵を保持する第 7 の鍵保持部 (1 5 1 2) と、

前記第 4 の復号処理部 (1 5 1 0) の出力を受けて、前記第 7 の鍵保持部に保

持された前記共通秘密鍵によって前記第1の再生情報を復号し、前記ライセンスキー(Kc)を抽出して前記コンテンツデータ再生部(1516, 1518)に対して出力するための第7の復号処理部(1514)をさらに有する、請求項20記載のデータ配信システム。

5 29. 前記コンテンツ供給装置(10)は、

前記コンテンツデータ再生部にて再生可能な第4の公開暗号鍵を保持する第7の鍵保持部と、

前記ライセンスキーを少なくとも含む前記第1の再生情報を前記第4の公開暗号鍵にて暗号化し、前記第1のライセンスデータ暗号化処理部に対して出力する
10 第3のライセンスデータ暗号化部をさらに含み、

前記コンテンツ再生部(1550)は、

前記第4の公開暗号鍵によって暗号化された前記第1の再生情報を復号できる第4の秘密復号鍵を保持する第7の鍵保持部と、

前記第4の復号処理部(1510)の出力を受けて、前記第7の鍵保持部に保持された前記第4の秘密復号鍵によって前記第1の再生情報を復号し、前記ライセンスキーを抽出して前記コンテンツ再生部に対して出力する第7の復号処理部
15 をさらに有する、請求の範囲第20項に記載のデータ配信システム。

30. データ配信システムであって、

暗号化コンテンツデータ({Data} Kc)と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ(Data)を得るための復号鍵であるライセンス
20 キー(Kc)とを配信するためのコンテンツ供給装置(10, 11)と、

前記コンテンツ供給装置(10, 11)からの前記配信を受ける複数の端末(100, 101)とを備え、

前記コンテンツ供給装置(10, 11)は、

25 外部との間でデータを授受するための第1のインタフェース部(350)と、

認証鍵(KPma)によって復号することで認証可能な状態に暗号化されたクラス証明データ(Cmc(m))を、前記第1のインタフェース部から受け取って前記認証鍵によって復号処理するための認証処理部(312)と、

前記暗号化コンテンツデータの配信の許可対象である前記クラス証明データを

リストアップした許可クラスリストを保持する許可クラスリスト保持部と、
前記認証処理部において得られた前記クラス証明データが前記許可クラスリスト保持部に保持される前記許可クラスリストに含まれる場合には、少なくとも前記ライセンスキーの配信動作を実行する配信制御部（３１５）とを含み

5 各前記端末（１００，１０１）は、
外部との間でデータを授受するための第２のインタフェース部（１１０２）と、
少なくとも前記ライセンスキーを受けて記録する配信データ解読部（１１０，
１１５）とを含み、

前記クラス証明データは、前記配信データ解読部に対応して定められ、
10 前記配信データ解読部は、
前記認証鍵によって復号することで正当性を証明できる状態に暗号化された前記クラス証明データを保持し、前記ライセンスキーを受信する場合に、前記第２のインタフェース部を介して出力する認証データ保持部（１４００）と、

前記暗号化コンテンツデータおよび前記ライセンスキーを記録するための第１
15 の記憶部（１４１５，１４４０）とを有する、データ配信システム。

３１． 前記配信データ解読部（１１０，１１５）は、前記端末（１００，１０１）に着脱可能な記録装置であり、

前記クラス証明データ（Cmc(m)）は、前記記録装置の種類ごとに対応して予め定められ、

20 前記配信データ解読部（１１０，１１５）は、
前記許可クラスリストを保持するための第２の記憶部と、
前記配信動作が指示されるのに応じて、前記第２の記憶部に保持される前記許可リストの更新を特定できる更新情報を生成する制御部（１４２０）とをさらに有し、

25 前記制御部は、前記更新情報を前記第２のインタフェース部（１１０２）を介して前記コンテンツ供給装置（１０，１１）に対して出力し、

前記コンテンツ供給装置は、前記第１のインタフェース部（３５０）を介して前記更新情報を受けて、前記配信制御部（３１５）へ与え、

前記配信制御部は、前記更新情報に基づいて、前記許可クラスリストを新しい

許可クラスリストに更新するための更新データを作成して、前記第1のインタフェース部を介して前記更新データを出力し、

5 前記制御部は、前記第2のインタフェース部(1102)を介して前記更新データを受けて、前記更新データに基づいて、前記第2の記憶部に保持される前記許可クラスリストの内容を更新する、請求の範囲第30項に記載のデータ配信システム。

32. 暗号化コンテンツデータ(Data)Kcと、前記暗号化コンテンツデータを復号して平文のコンテンツデータ(Data)を得るための復号鍵であるライセンスキー(Kc)とを受けて記録するための記録装置であって、

10 外部との間でデータを授受するためのインタフェース部(1202)と、
認証鍵(KPma)によって復号することで認証可能な状態に暗号化された、前記記録装置に対応して定められる、第1のクラス証明データ(Cmc(m))および第1の公開暗号鍵(KPmc(m))を保持し、前記暗号化コンテンツデータを受信する場合において前記インタフェース部を介して外部に出力する認証データ保持部(1
15 400)と、

前記第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵(Kmc(m))を保持する第1の鍵保持部(1402)と、

前記第1の公開暗号鍵によって暗号化された第1の共通鍵(Ks1)を前記インタフェース部を介して外部から受けて、復号処理するための第1の復号処理部
20 (1404)と、

前記記録装置ごとに異なる第2の公開暗号鍵(KPm(i))を保持する第2の鍵保持部(1416)と、

前記コンテンツデータの通信ごとに更新される第2の共通鍵(Ks2)を生成するセッションキー発生部(1418)と、

25 前記第2の共通鍵および前記第2の公開暗号鍵を前記第1の共通鍵によって暗号化し、前記インタフェース部を介して外部に出力するための第1の暗号化処理部(1406)と、

前記インタフェース部を介して、前記第2の共通鍵および前記第2の公開暗号鍵によって暗号化された、少なくとも前記ライセンスキーを含む第1の再生情報

を受けて、前記第2の共通鍵によって復号するための第2の復号処理部（1412）と、

前記第2の公開暗号鍵によって暗号化されたデータを復号するための第2の秘密復号鍵（ $K_m(i)$ ）を保持する第3の鍵保持部（1421）と、

5 前記前記第2の秘密復号鍵による復号処理を実行するための第3の復号処理部（1422）と、

前記第1の再生情報および前記暗号化コンテンツデータを記録するための第1の記憶部（1415、1440）とを備える、記録装置。

33. 前記コンテンツデータの通信の禁止対象とされる前記第1のクラス証明データ（ $Cmc(m)$ ）をリストアップした禁止クラスリストを保持するための第2
10 の記憶部（1430、2415）と、

前記コンテンツデータの配信動作が指示されるのに応じて、前記インタフェース部（1202）を介して外部から受けた情報に基づいて、前記第2の記憶部に保持される前記リストの内容を更新することが可能な制御部（1420）と、

15 外部から指示される、他の記録装置（112、116）に対して、少なくとも前記第1の再生情報を含むデータを移転するための移動動作に応じて、前記他の記録装置から暗号化された前記第1のクラス証明データ（ $Cmc(m)$ ）を受けて、前記認証鍵（ $KPma$ ）による復号を行なって前記正当性を確認するための認証処理部（1408）とをさらに備え、

20 前記制御部は、前記移動動作時において、前記認証処理部において得られた前記他の記録装置に対応する前記第1のクラス証明データが前記第2の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記移動動作を中止する、請求の範囲第32項に記載の記録装置。

34. 認証処理部（1408）は、外部から指示される前記コンテンツデータの再生動作に応じて、前記認証鍵（ $KPma$ ）によって暗号化された、前記コンテンツデータの再生回路（1550）に対応する第2のクラス証明データ（ $Cp(n)$ ）を前記インタフェース部（1202）を介して受けて復号し、

25 前記禁止クラスリスト（CRL）は、禁止対象とされる前記第2のクラス証明データをさらにリストアップし、

前記制御部（１４２０）は、前記再生動作に応じて、前記認証処理部において得られた前記再生回路に対応する前記第２のクラス証明データが前記第２の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記再生動作を中止する、請求の範囲第３３項に記載の記録装置。

５ ３５． 前記第２の記憶部（１４３０，２１４５）は、第三者に読出不可能なセキュリティー領域（TRM）内に配置される、請求の範囲第３３項に記載の記録装置。

３６． 前記禁止クラスリスト（CRL）のデータを前記第２の公開暗号鍵（KP_{m(i)}）で暗号化するための第２の暗号化処理部（１４２４）をさらに備え、
１０ 前記第２の記憶部（２４１５）は、第三者に読出不可能なセキュリティー領域（TRM）外に設けられて、前記第２の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第３３項に記載の記録装置。

３７． 前記記録装置ごとに異なる秘密鍵（K(i)）を保持する秘密鍵保持部（１４５０）と、

１５ 前記秘密鍵による暗号化を実行するための、秘密鍵暗号化処理部（１４５２）と、

前記秘密鍵で暗号化されたデータを復号するための秘密鍵復号処理部（１４５４）とをさらに備え、

前記第１の記憶部（１４１５）および前記第２の記憶部（２４１５）は、第三者に読出不可能なセキュリティー領域（TRM）外に設けられ、
２０

前記第１の記憶部（１４１５）は、前記第２の暗号化処理部によって暗号化されたデータを保持し、

前記第２の記憶部（２４１５）は、前記第２の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第３３項に記載の記録装置。

２５ ３８． 前記第１の記憶部（１４１５，１４４０）は、半導体メモリであり、
前記記録装置は、メモリカードである、請求の範囲第３２項に記載の記録装置。

３９． 記録装置であって、

データ（K_c）を記録するための第１の記憶部（１４１５，１４４０）と、
インタフェース部（１２０２）を介して入力される、認証鍵(KP_{ma})によって

復号することで認証可能な状態に暗号化されたクラス証明データ (Cmc(m), Cp(n)) を受けて、前記認証鍵による復号を行なって正当性を確認するための認証処理部 (1408) と、

- 5 前記データの出力を許可する対象となされるクラス証明データをリストアップした許可クラスリストを保持するための第2の記憶部と、

外部からの前記データの出力指示に応じて、前記インタフェース部を介した前記データの出力を制御する制御部 (1420) とを備え、

- 10 前記制御部は、前記出力指示とともに外部から前記インタフェース部を介して入力される、前記暗号化がなされた前記クラス証明データを前記認証処理部で復号して得られる前記クラス証明データが前記許可クラスリストに含まれる場合において、前記データの出力を実行する、記録装置。

FIG.1

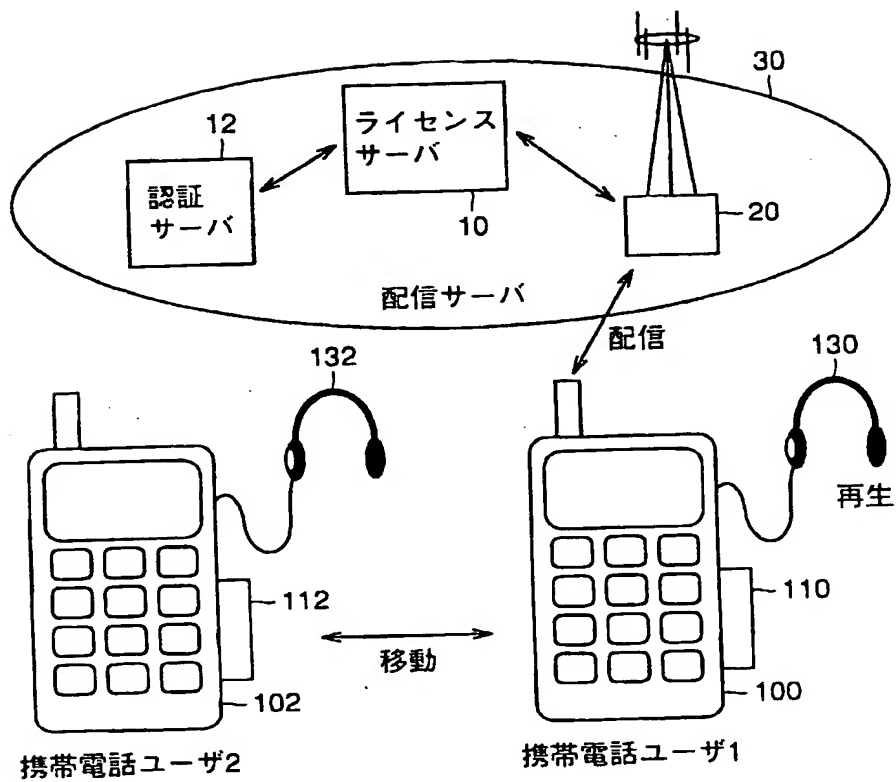


FIG.2

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいは サーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数、機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報 (例：再生可否)

FIG.3

名称	属性	保持/発生箇所	機能・特徴
CRL	禁止クラスリスト 関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 (差分データ形式)
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPp(n)	公開暗号化鍵 (非対称鍵)	携帯電話機	Kp(n)にて復号可能。 (KPp(n)//Cp(n))KPmaの形式で出荷時に記録 *携帯電話機の種類ごと(n)に異なる情報を有する。
KPmc(m)	公開暗号化鍵 (非対称鍵)	メモリカード	Kmciにて復号可能。 (KPmc(m)//Cmc(m))KPmaの形式で出荷時に記録 *メモリカードの種類ごと(m)に異なる情報を有する。
Kp(n)	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 *携帯電話機の種類ごと(n)に異なる情報を有する。
Kmc(m)	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 *メモリカードの種類ごと(m)に異なる情報を有する。
Cp(n)	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 (KPp(n)//Cp(n))KPmaの形式で出荷時に記録 *携帯電話機の種類ごと(n)に異なる情報を有する。
Cmc(m)		メモリカード	メモリカードのクラス証明書。認証機能を有する。 (KPmc(m)//Cmc(m))KPmaの形式で出荷時に記録 *メモリカードの種類ごと(m)に異なる情報を有する。

FIG.4

名称	属性	保持/発生箇所	機能・特徴
Ks1	共通鍵 (セッション固有)	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信/移動(受)セッション毎に発生
Ks3		メモリカード	再生/移動(送)セッション毎に発生
Ks4		携帯電話機	再生セッション毎に発生
Km(i)	秘密復号鍵	メモリカード	メモリカードごと(i)に固有の復号鍵 Kpm(i)で暗号化されたデータはKm(i)で復号可能
Kpm(i)	公開暗号化鍵 (非対称鍵)	メモリカード	メモリカードごと(i)に固有の暗号化鍵
KPma	復号鍵	配信サーバ	配信システム全体で共通。
Kcom	秘密復号鍵	携帯電話機 配信サーバ	再生回路共通の秘密鍵。Kc,AC2の暗号化および復号 に利用。

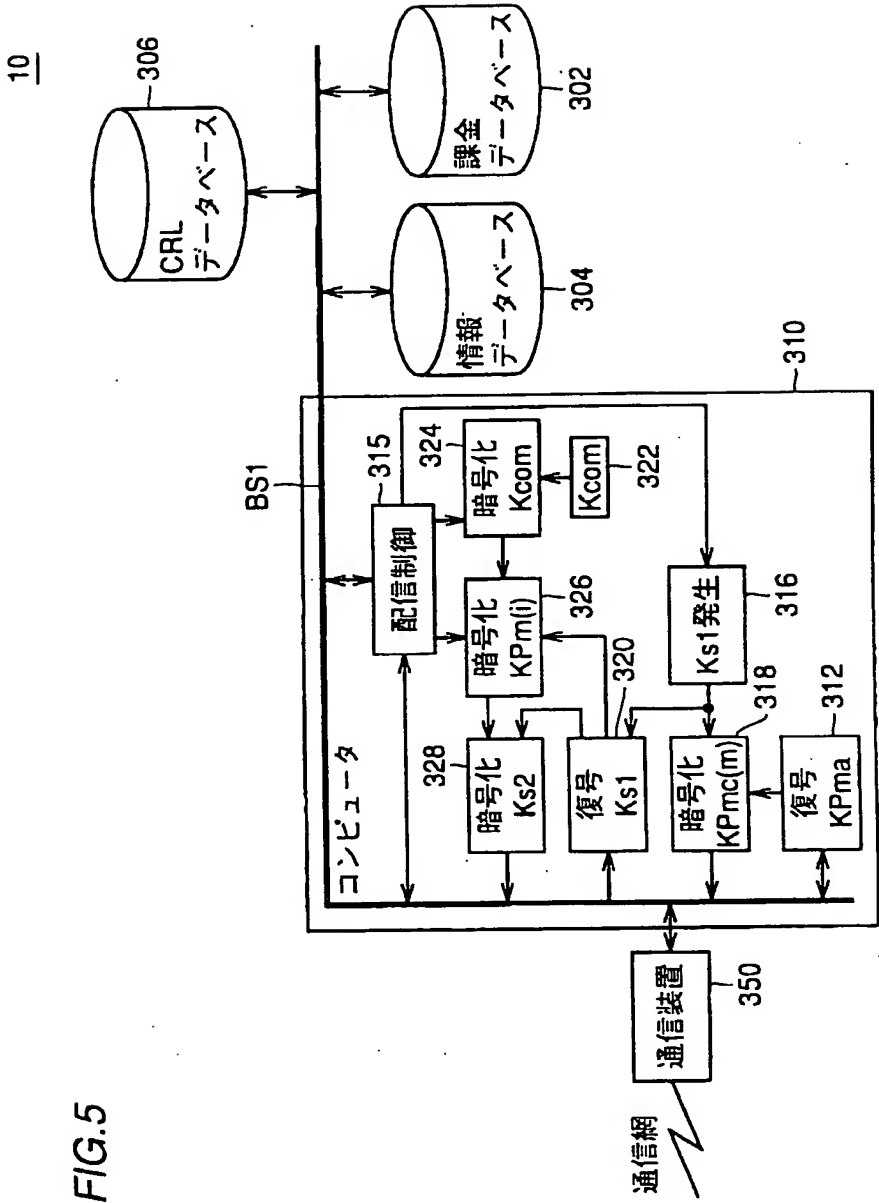


FIG.6

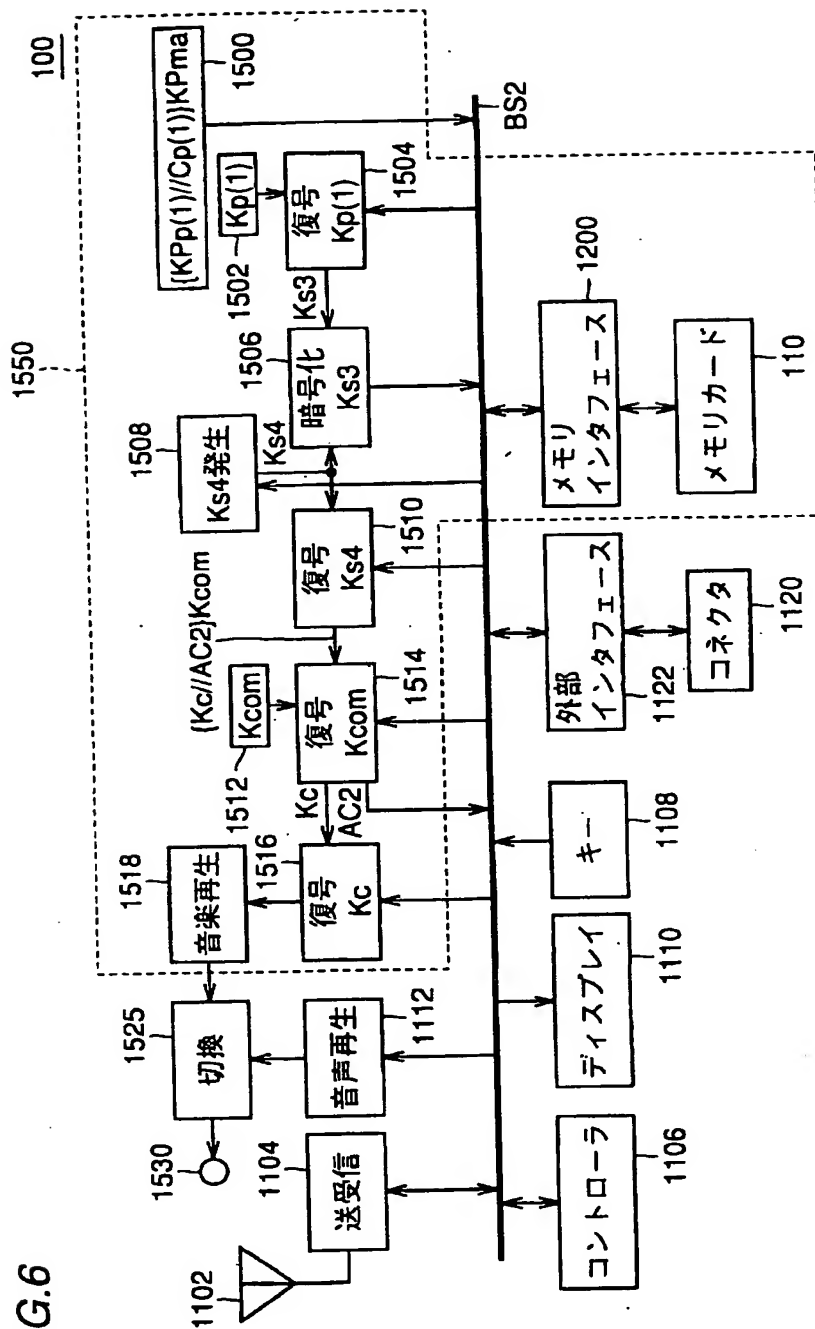


FIG. 7

110

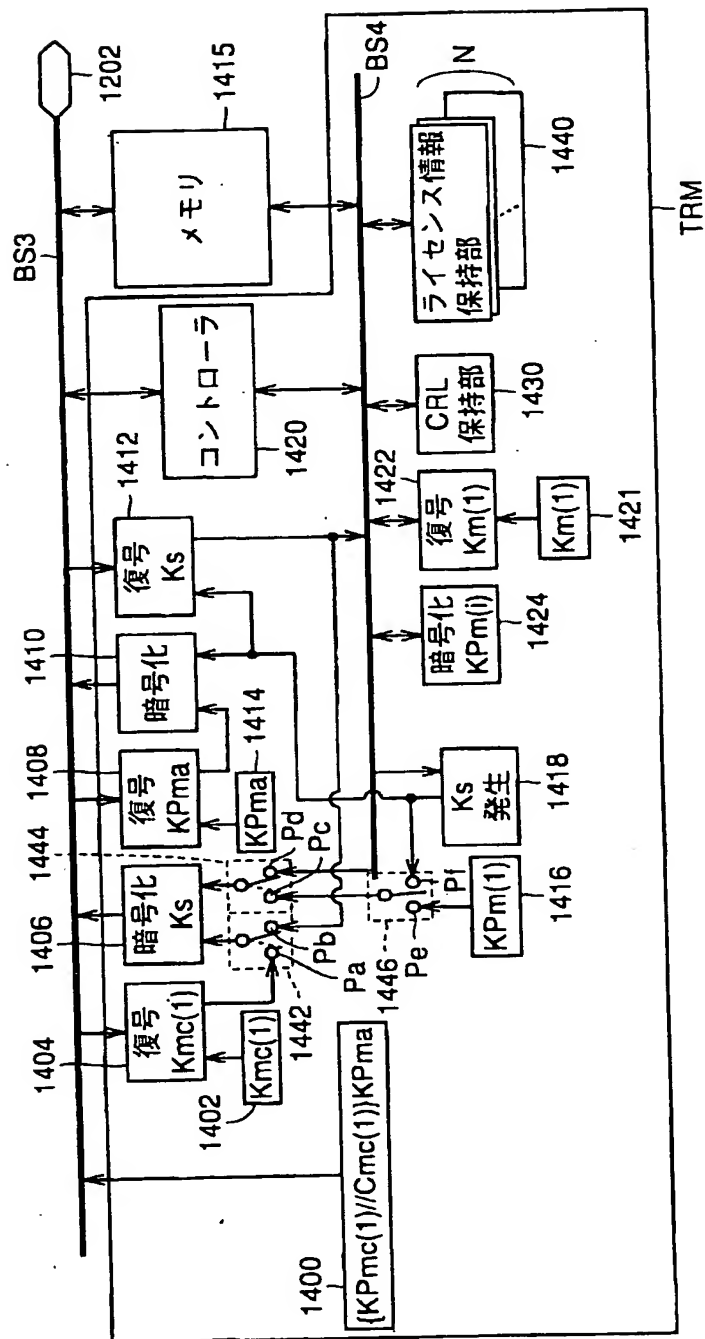


FIG. 8

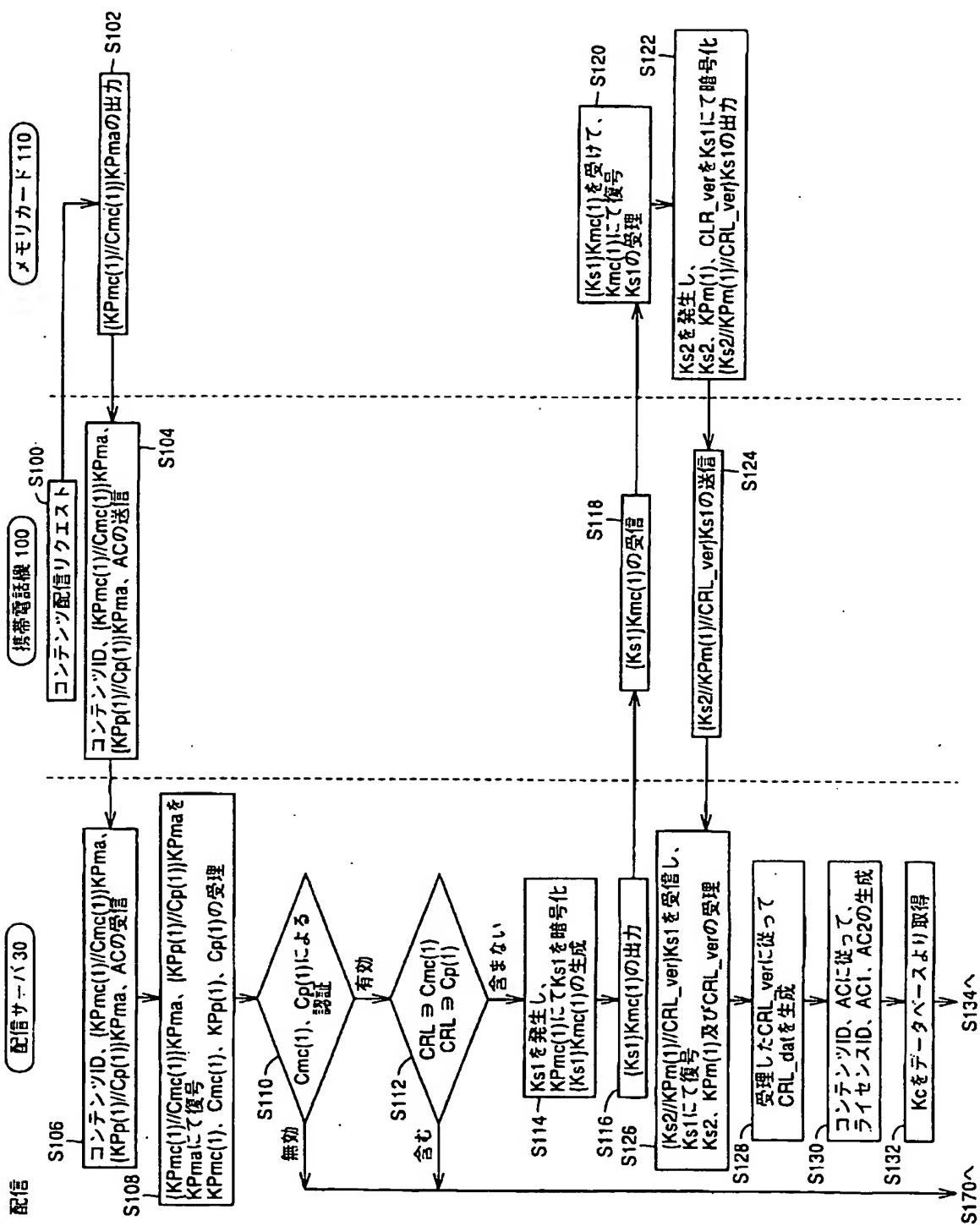


FIG.9

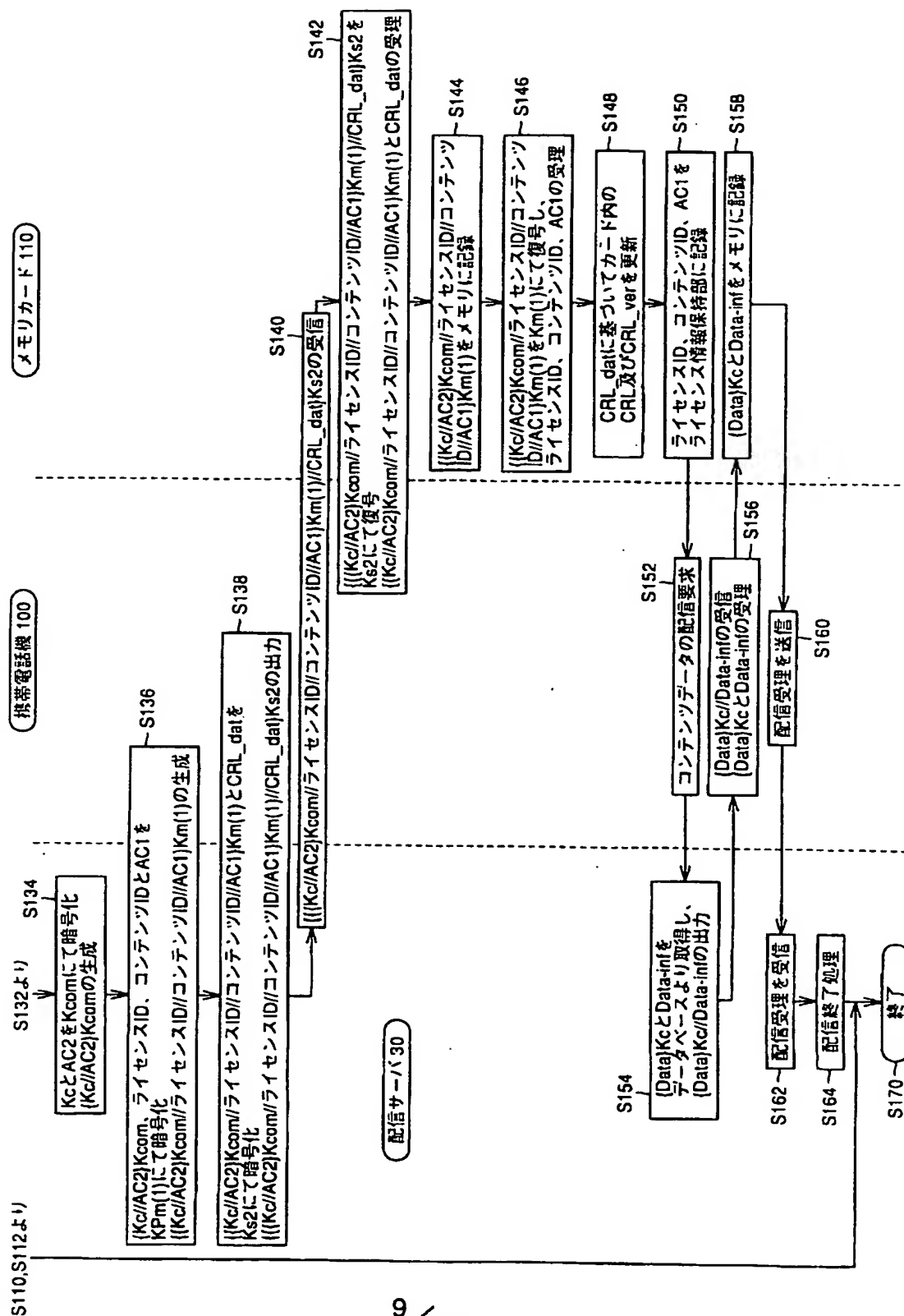
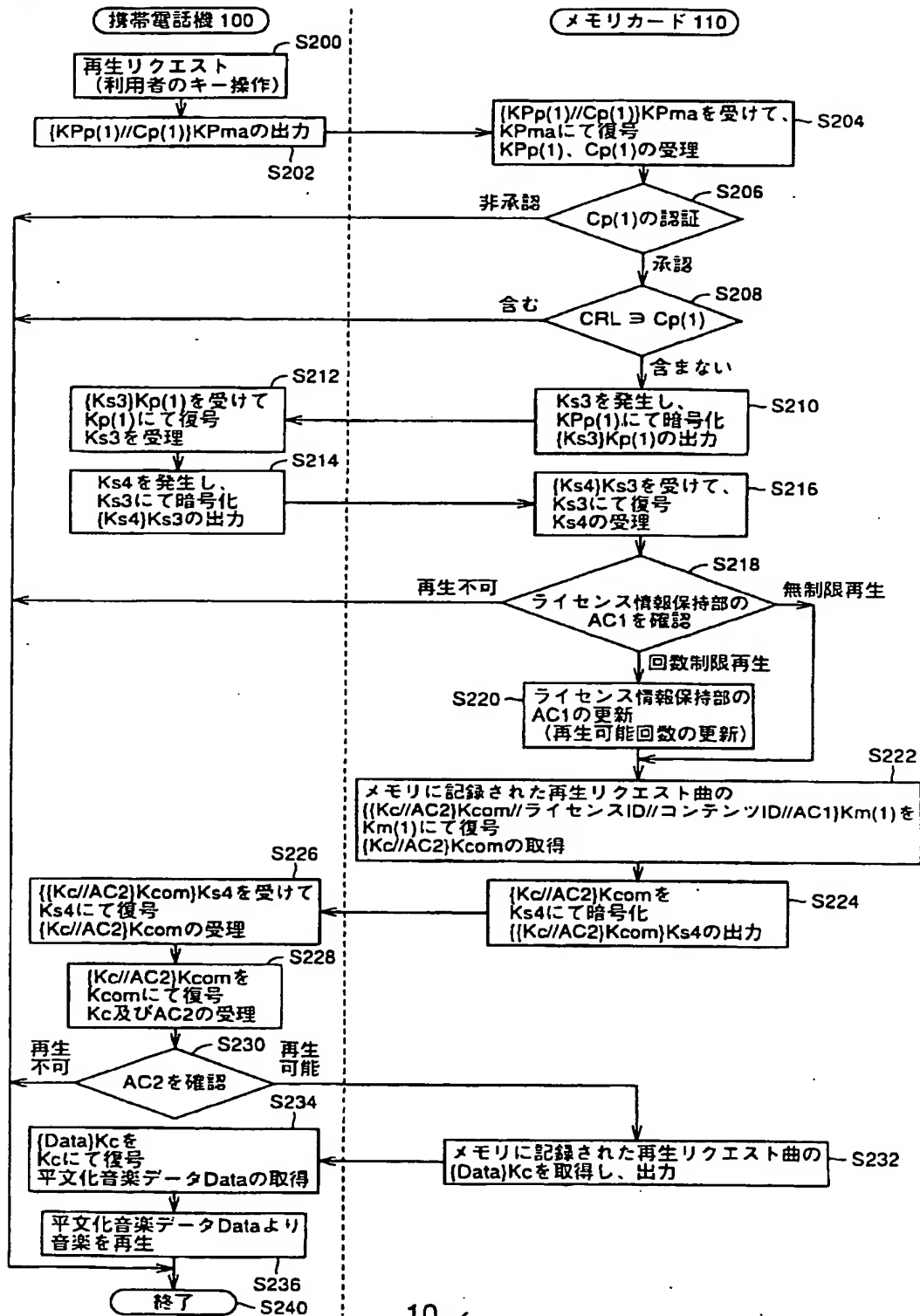


FIG. 10

再生



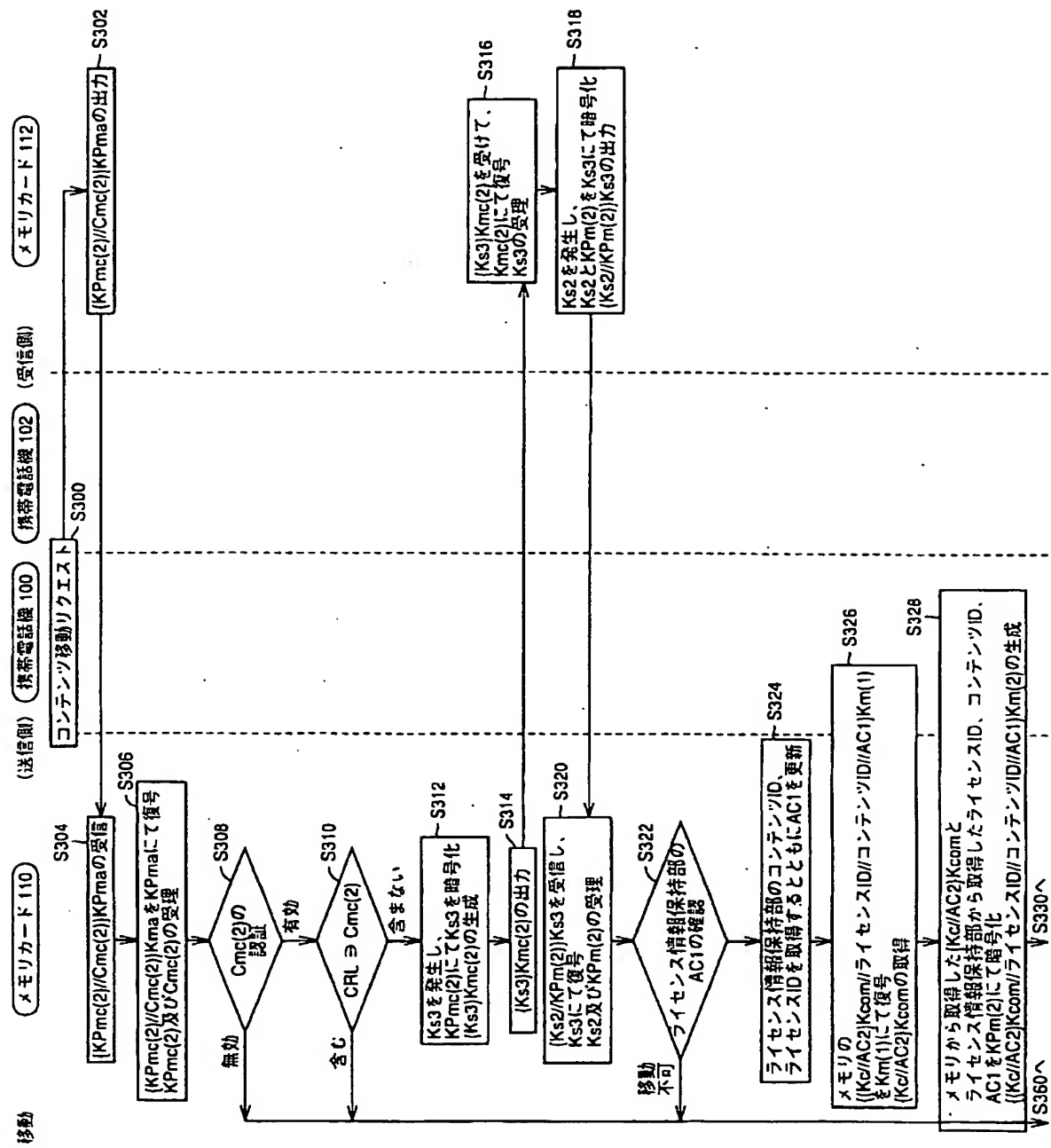


FIG. 12

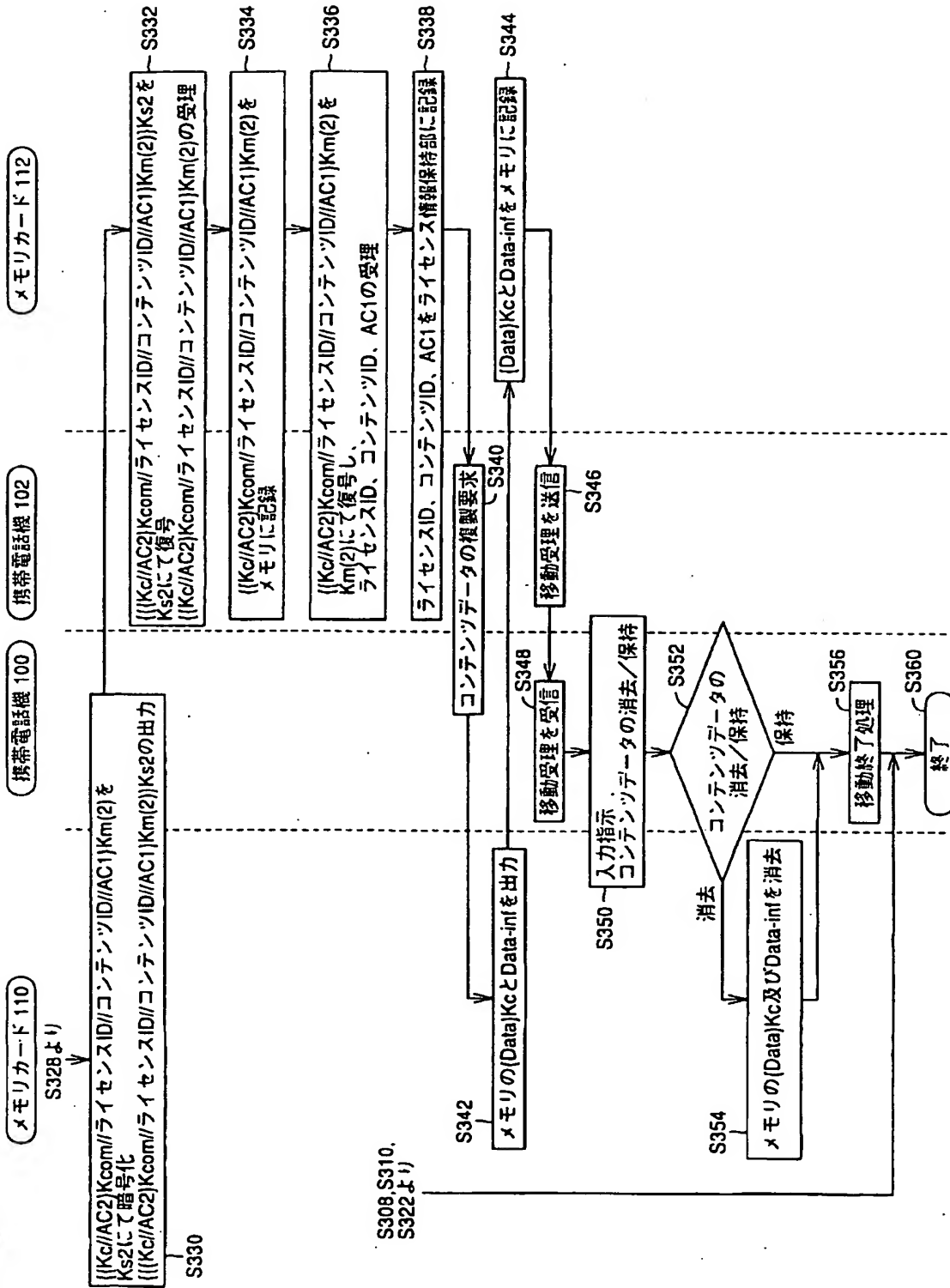


FIG.13

11

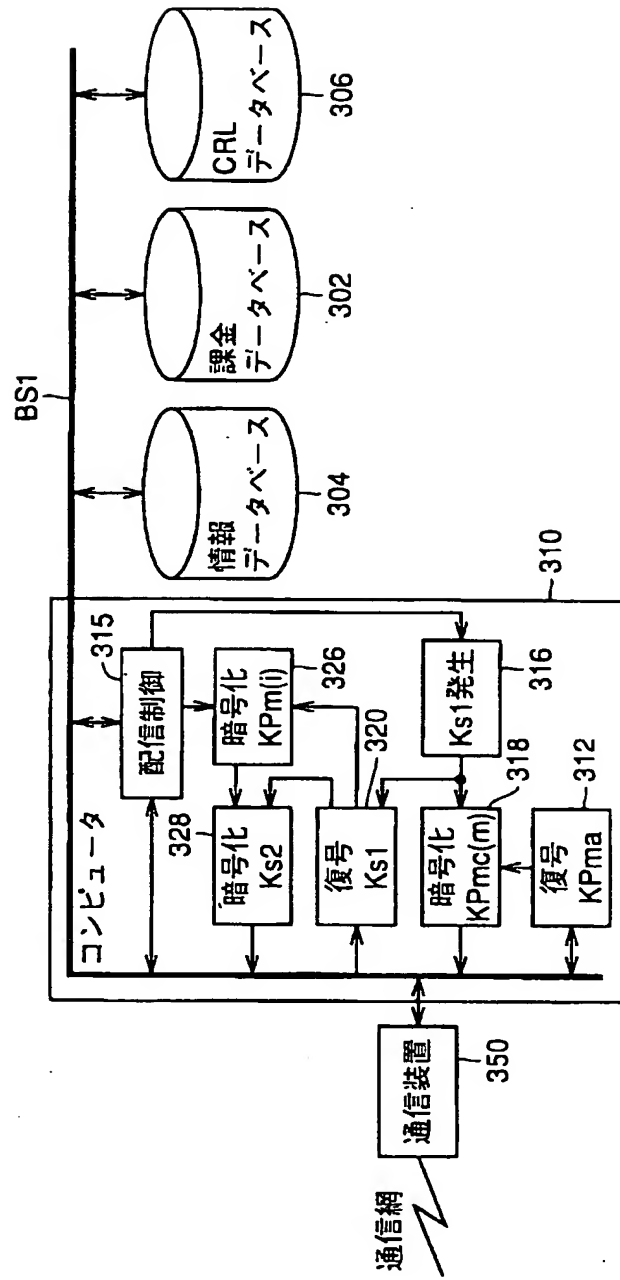


FIG. 14

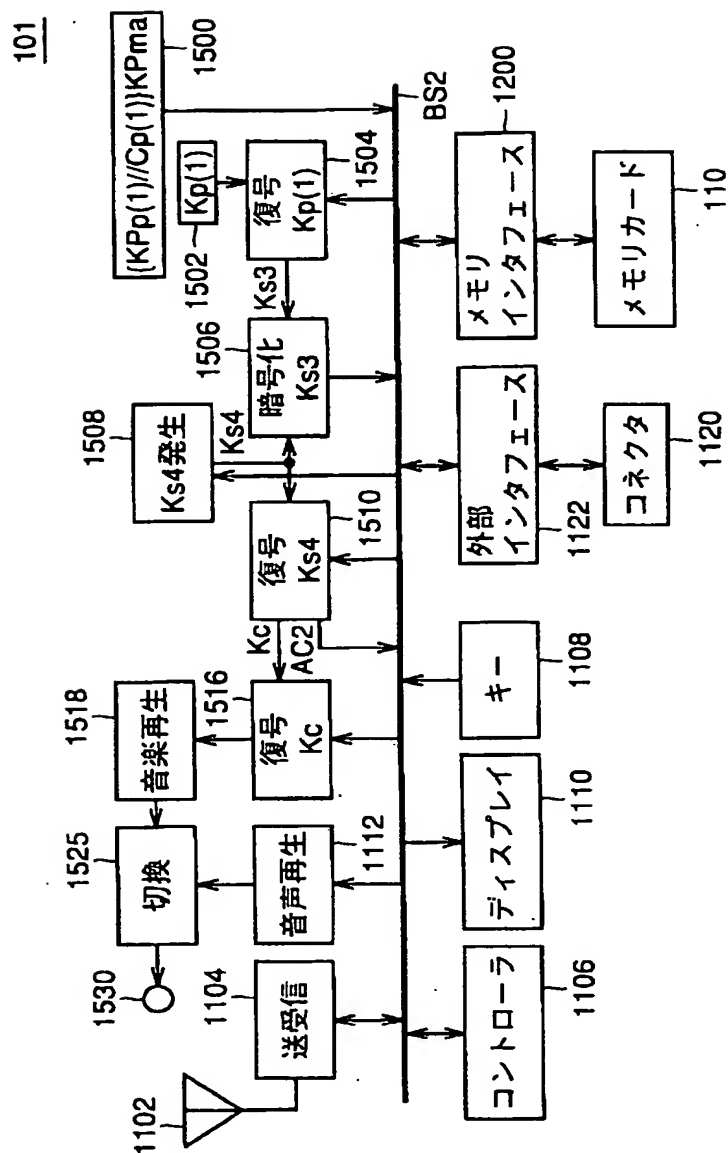


FIG.15

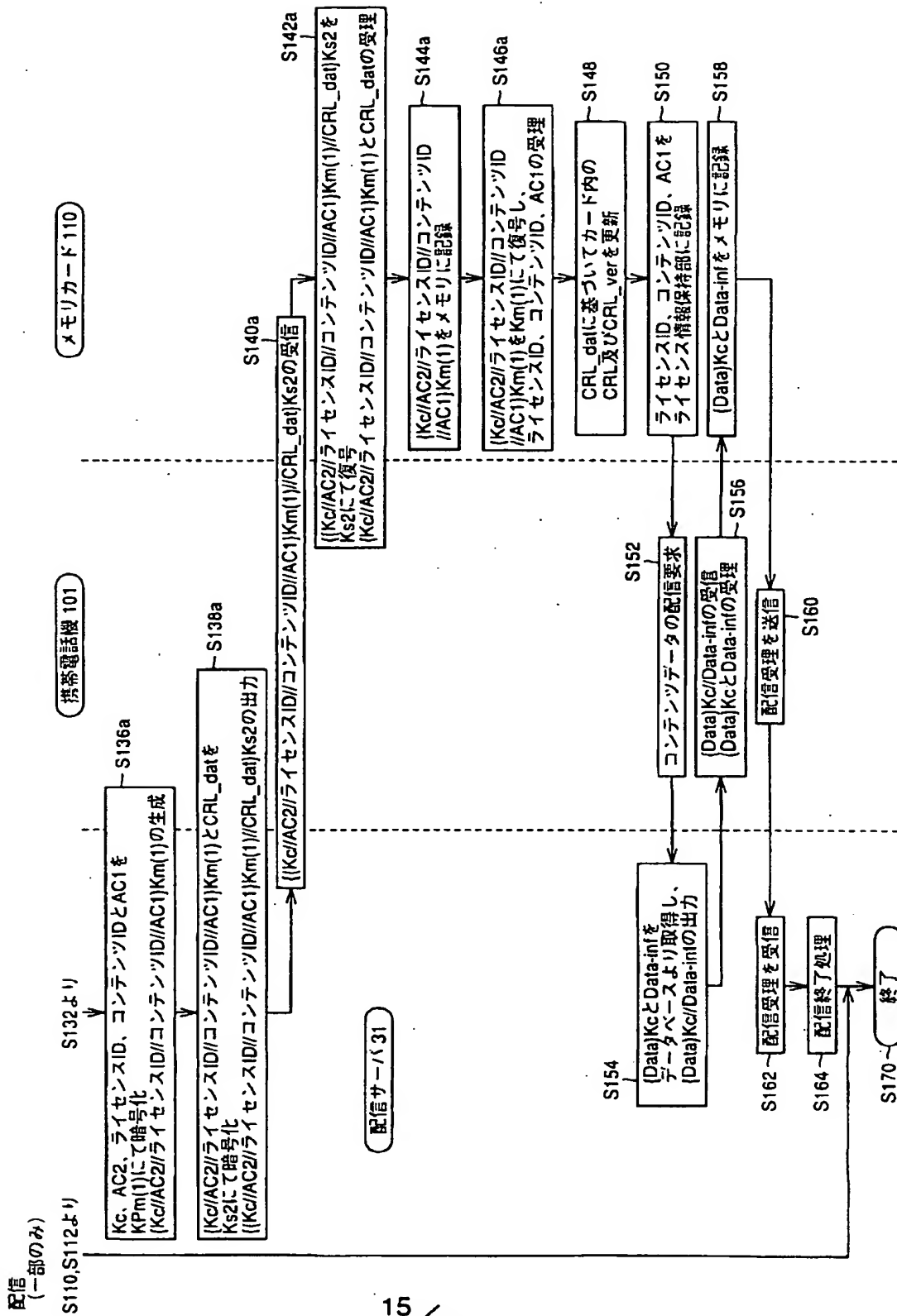


FIG. 16

再生

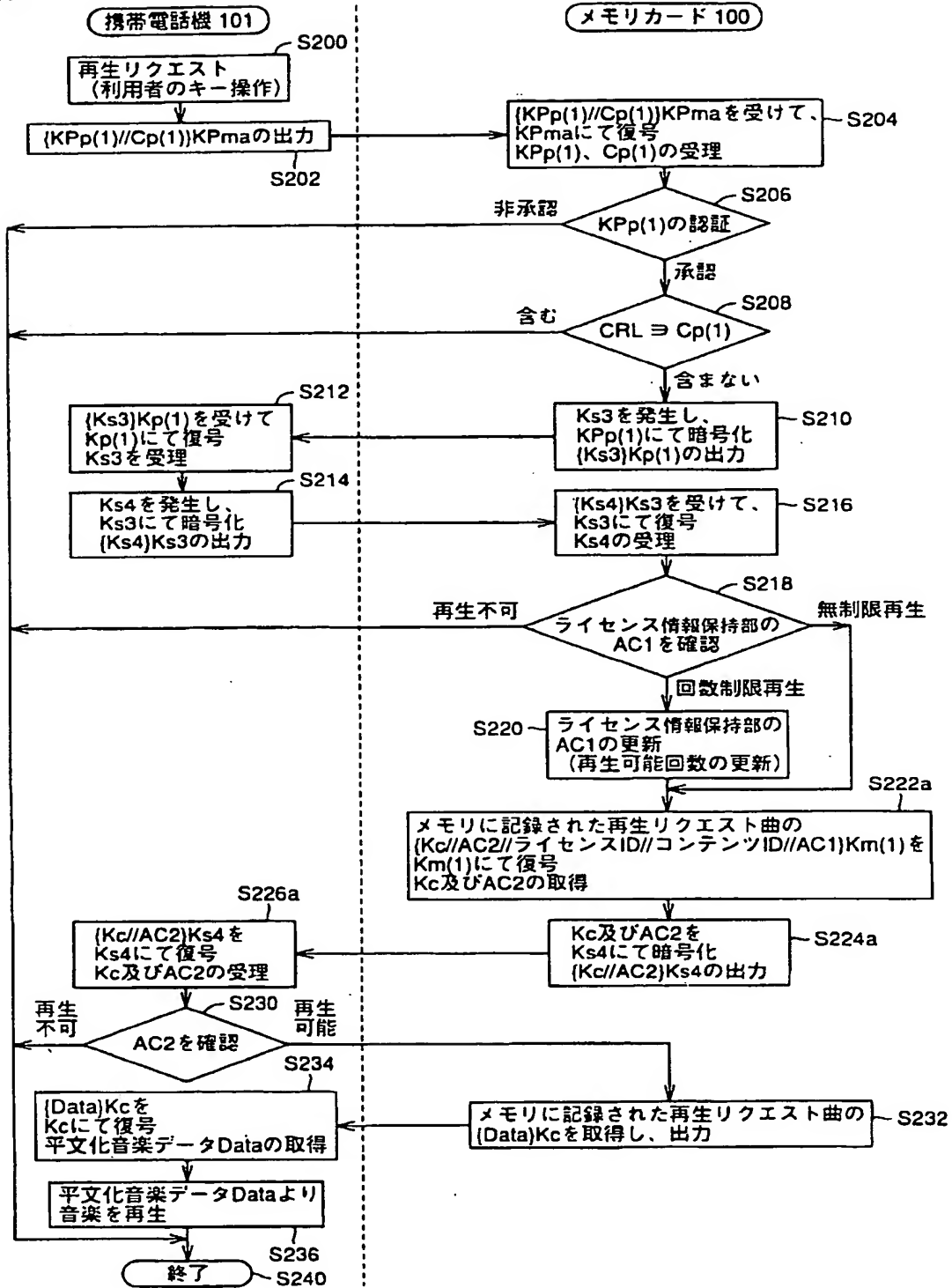


FIG. 17

移動

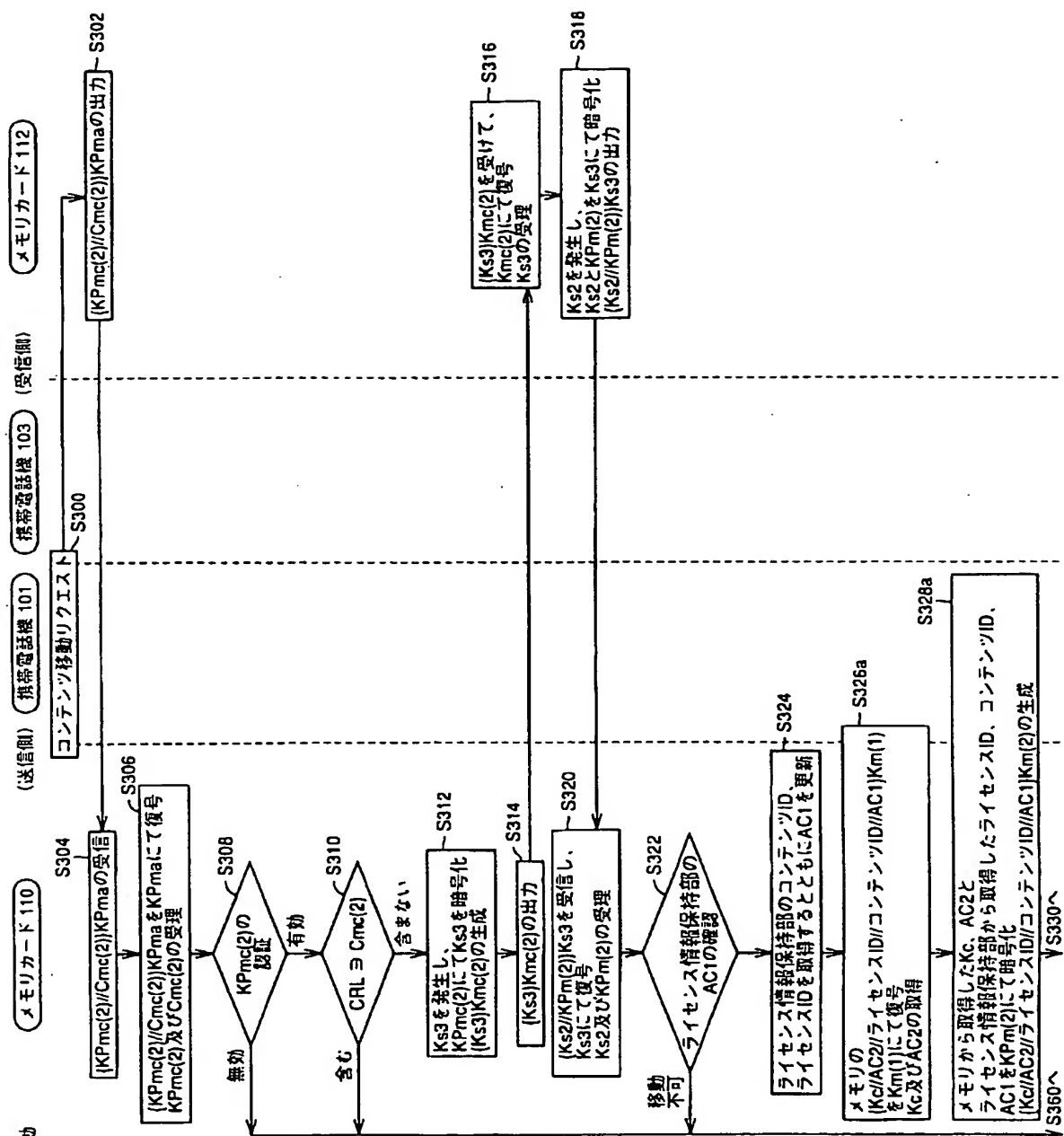


FIG. 18

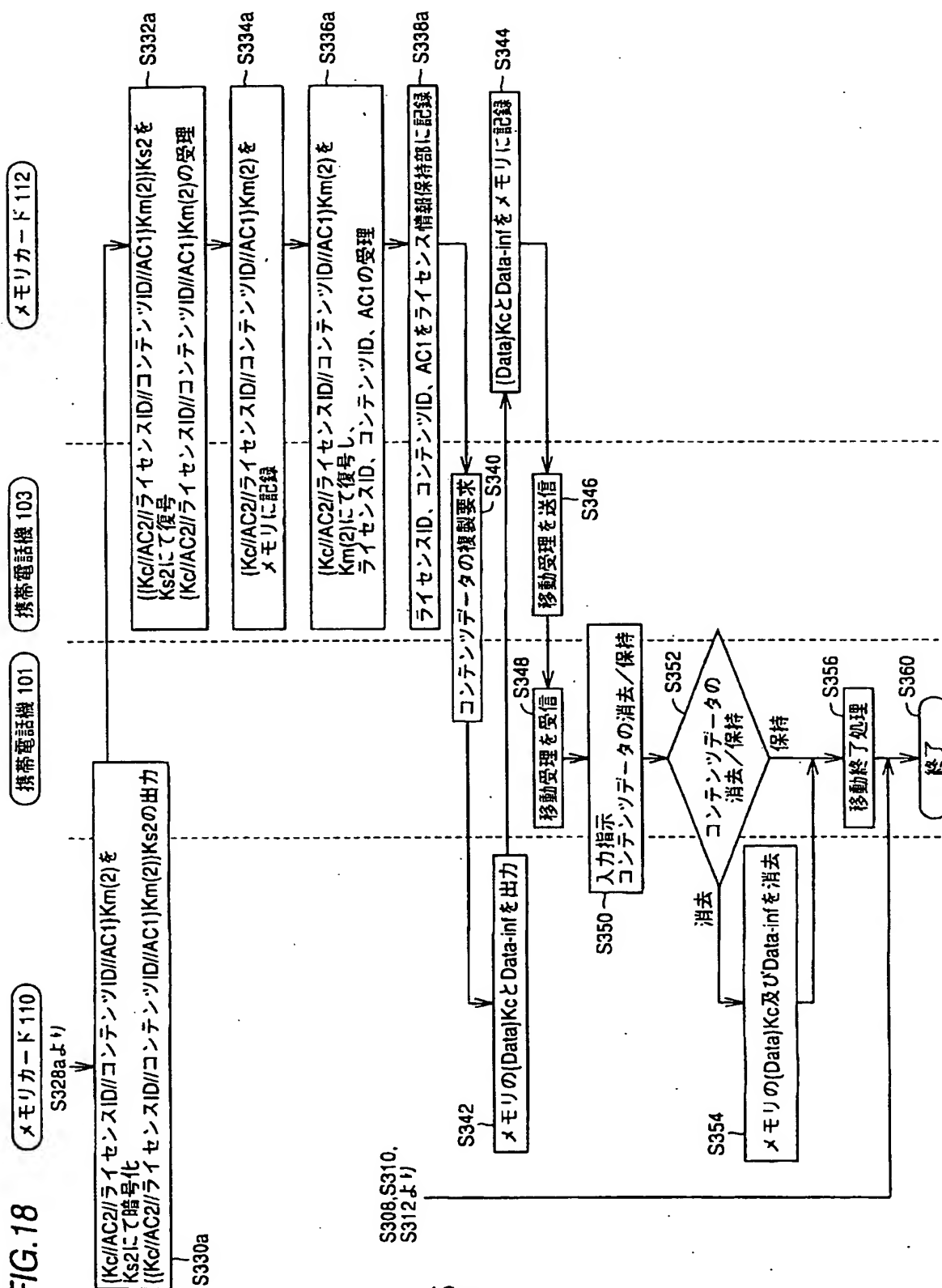


FIG. 19

115

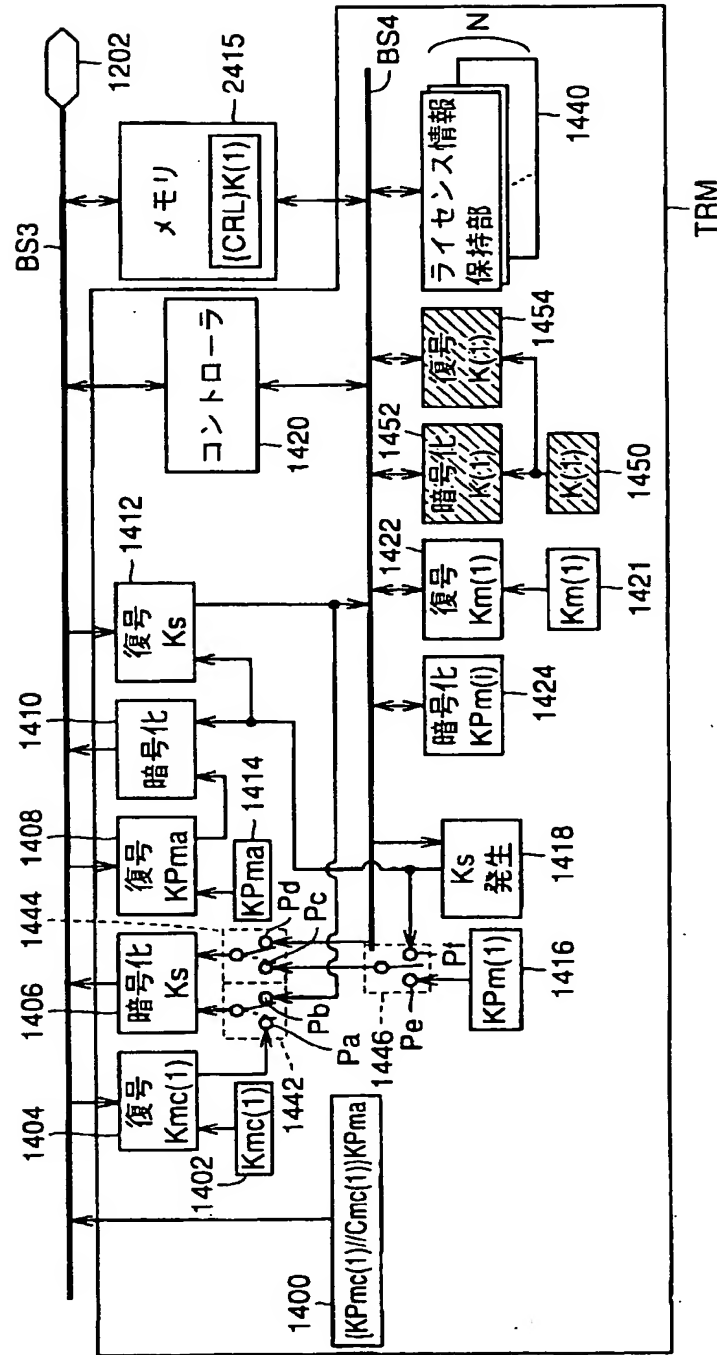


FIG.20

名称	属性	保持/発生箇所	機能・特徴
Ks1	共通鍵 (セッション固有)	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信/移動(受)セッション毎に発生
Ks3		メモリカード	再生/移動(送)セッション毎に発生
Ks4		携帯電話機	再生セッション毎に発生
Km(i)	秘密復号鍵	メモリカード	メモリカードごと(i)に固有の復号鍵 KPM(i)で暗号化されたデータはKm(i)で復号可能
KPM(i)	公開暗号化鍵 (非対称鍵)	メモリカード	メモリカードごと(i)に固有の暗号化鍵
KPma	公開復号鍵	配信サーバ	配信システム全体で共通。
Kcom	秘密共通鍵	携帯電話機	再生回路共通の秘密鍵。Kc, AC2の暗号化および復号に利用。
K(i)	秘密鍵 (対称鍵)	メモリカード	メモリカードごとに固有の秘密鍵 (i)はメモリカードを識別する引数 対称鍵なので高速に復号可能

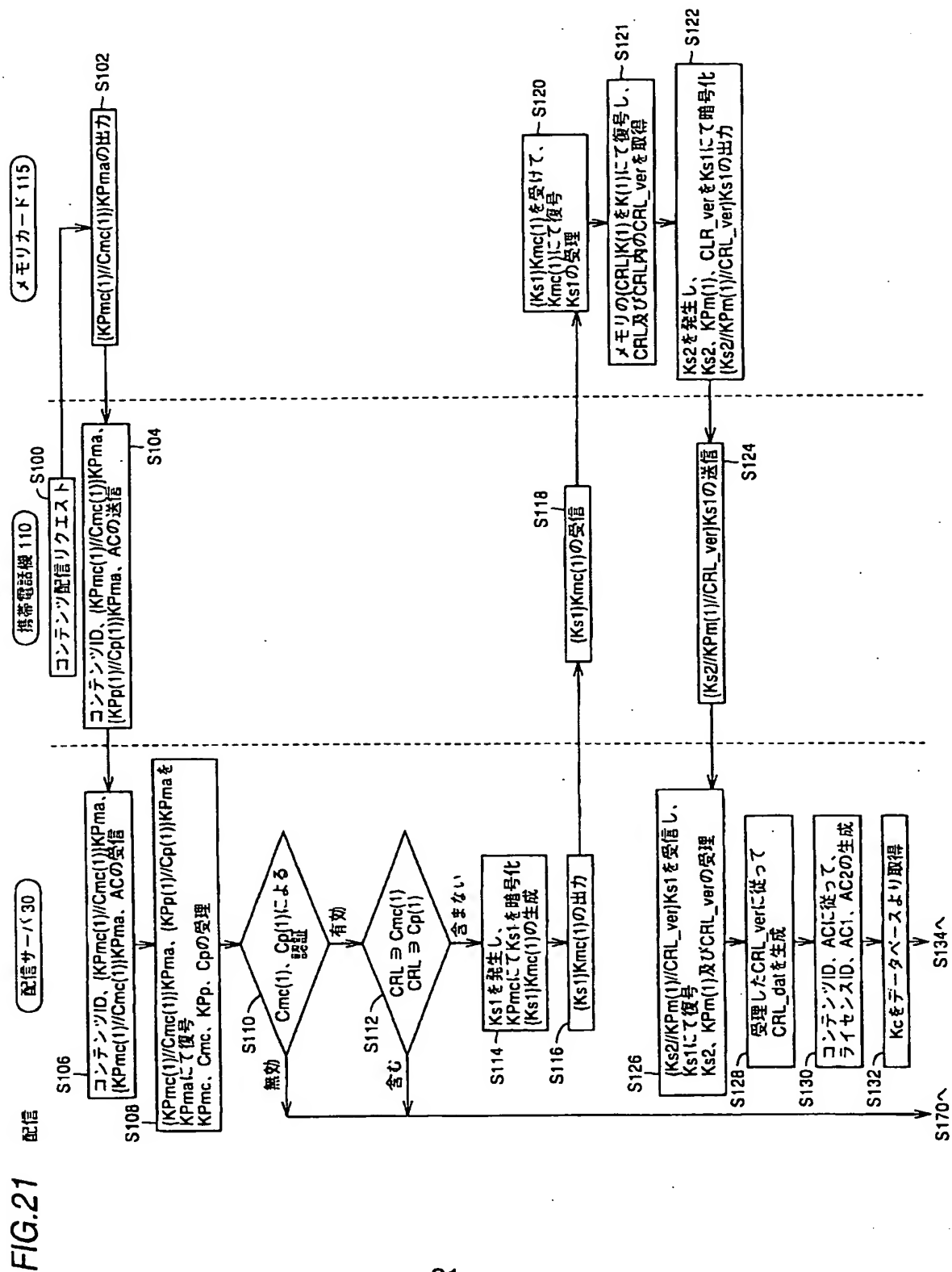


FIG.22

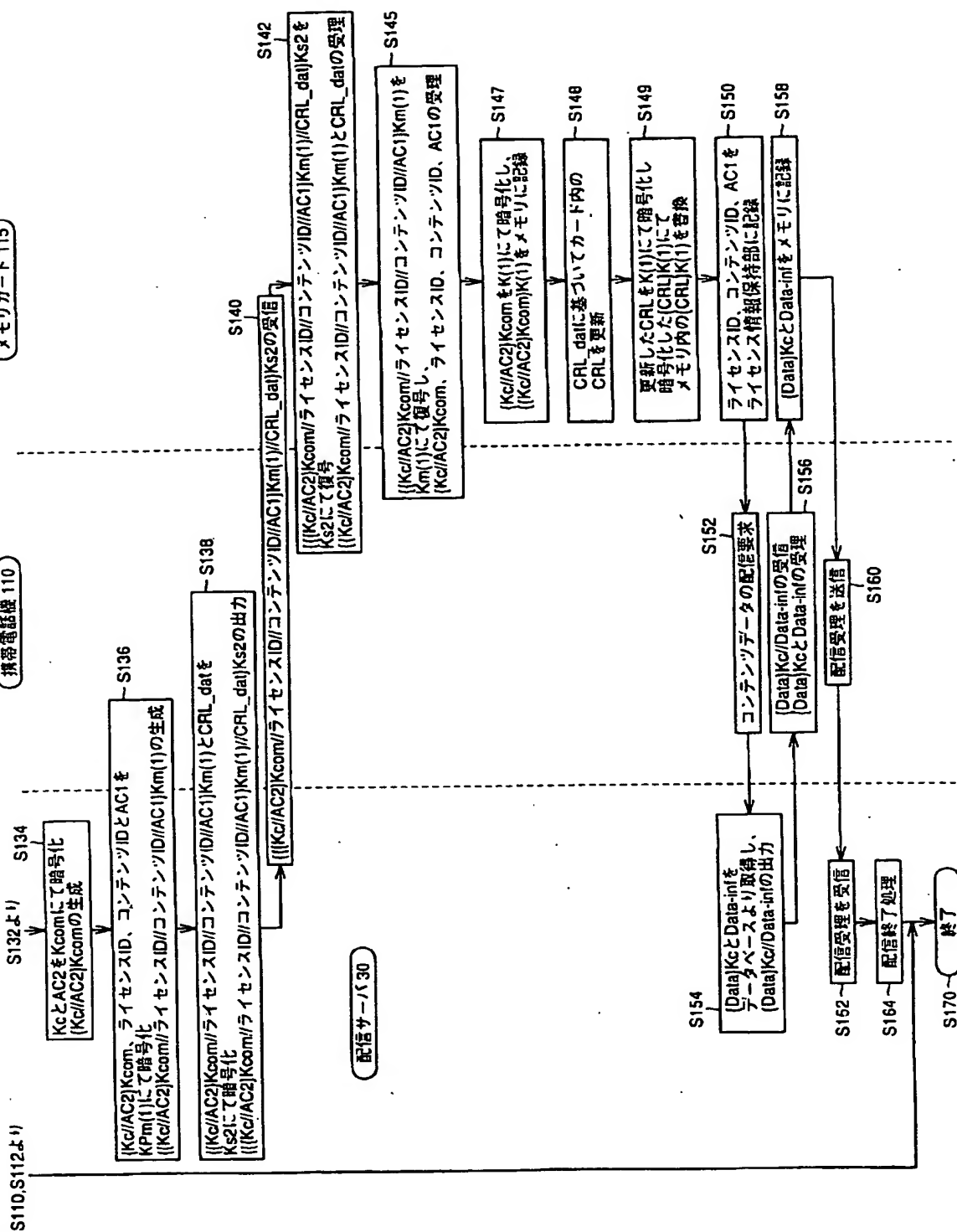
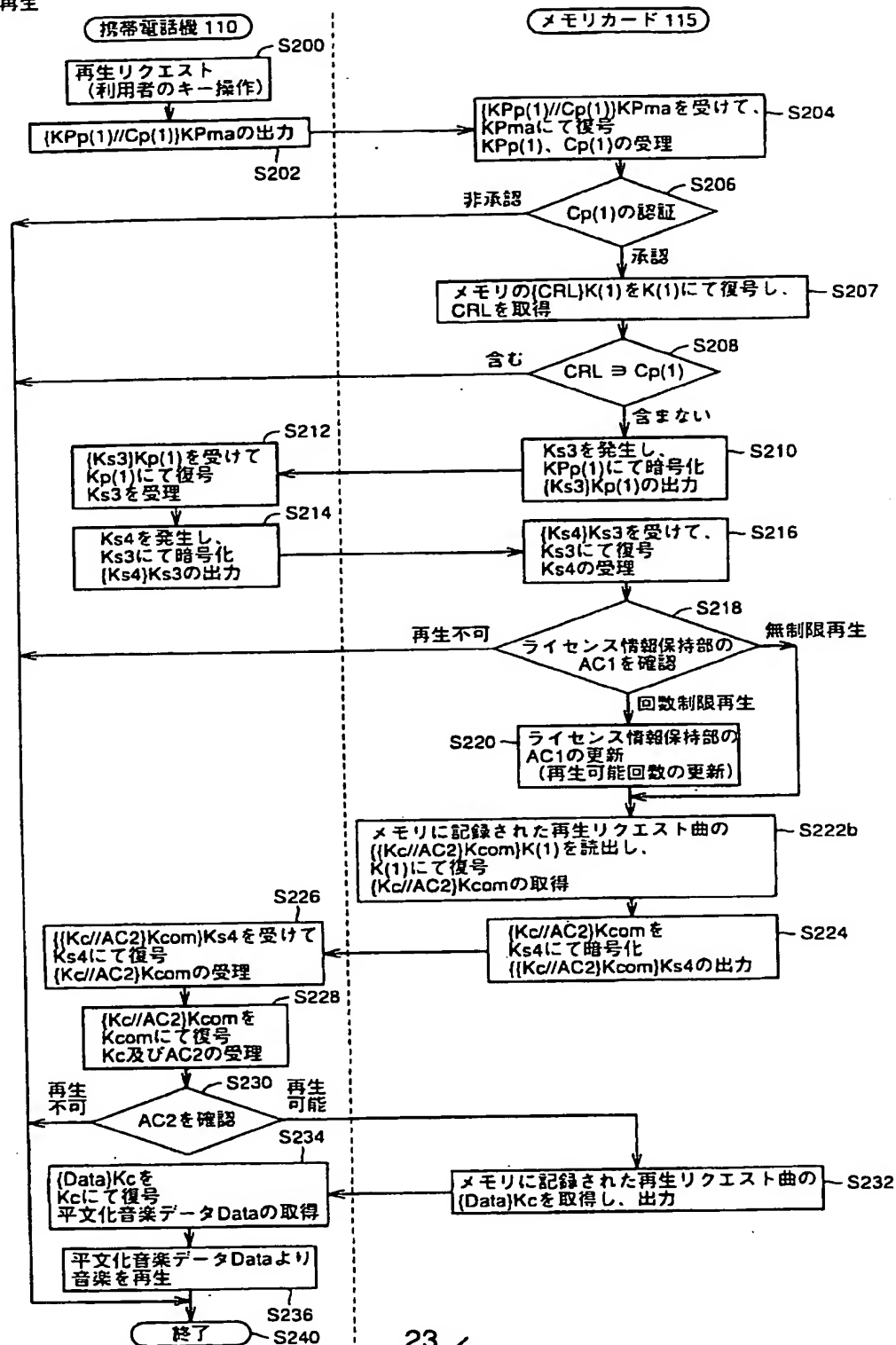


FIG.23

再生



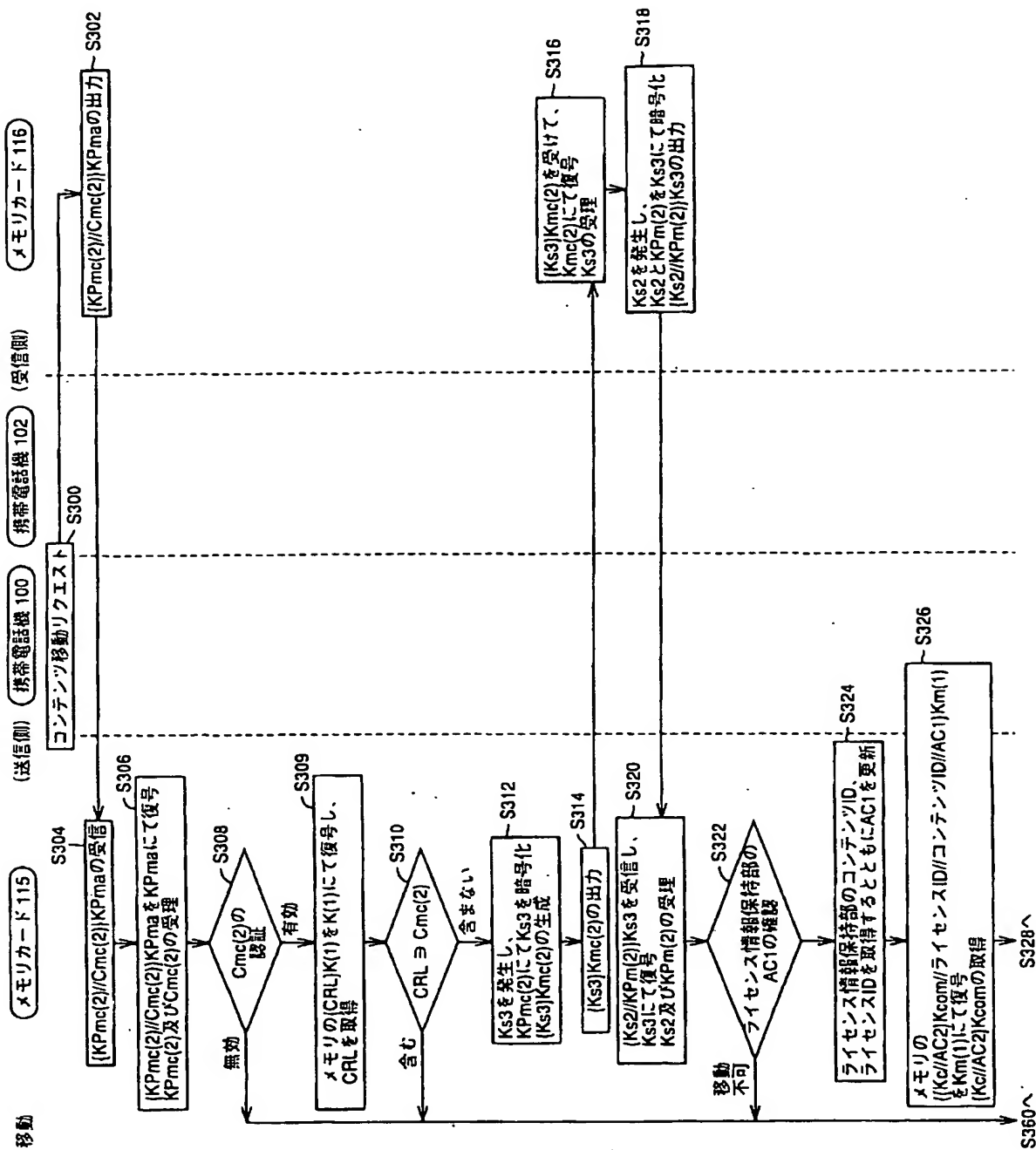
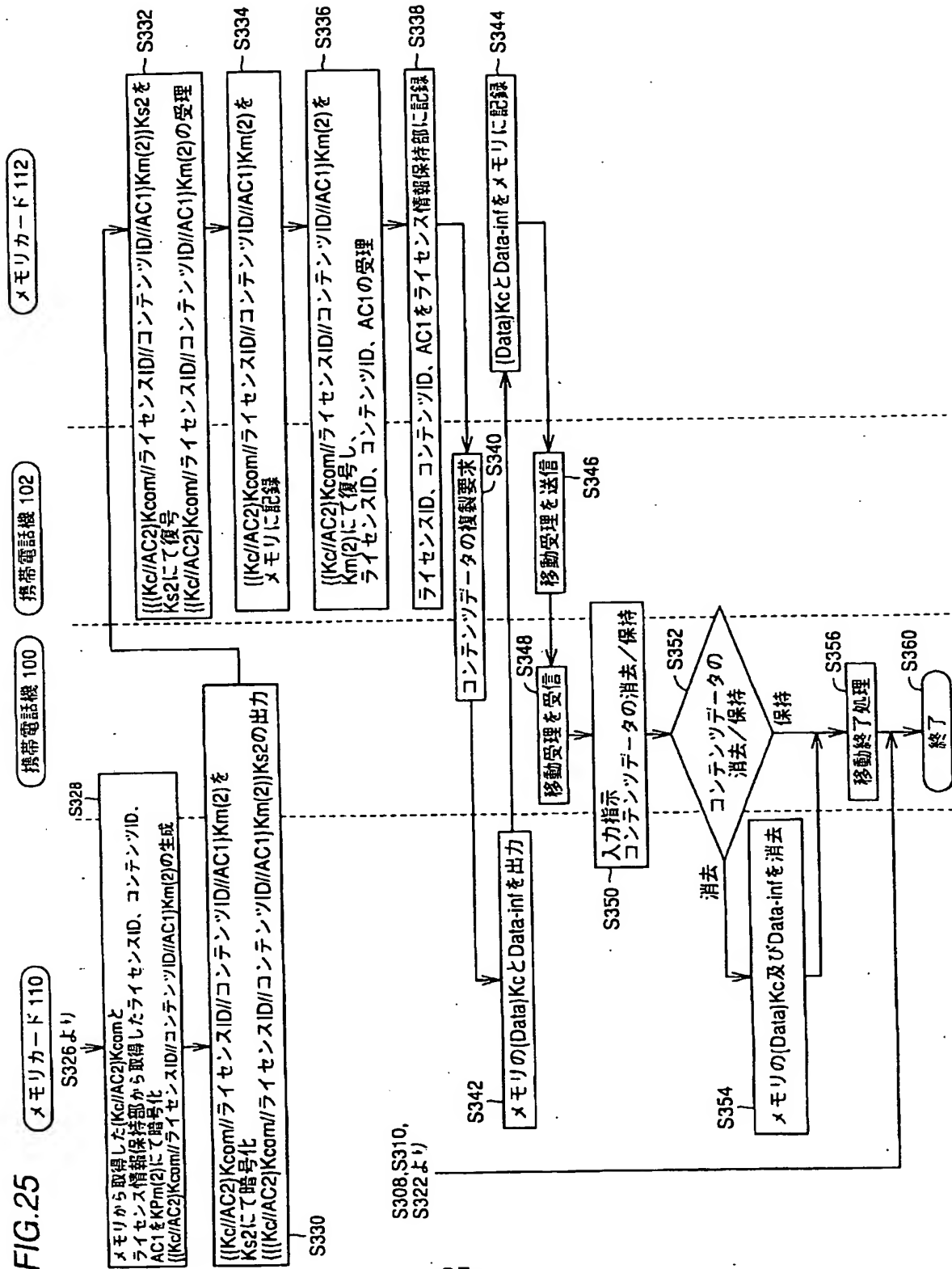


FIG. 25



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/08497

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS)
WPI (DIALOG)
INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Digital Transmission Content Protection Specification, Volume 1 (Informational Version), Revision 1.0, (1999 April)	1-39
EA	JP, 2000-357127, A (Toshiba Corporation), 26 December, 2000 (26.12.00) (Family: none)	1-39
A	JP, 6-326786, A (Hitachi Denshi, Ltd.), 25 November, 1994 (25.11.94) (Family: none)	1-39
A	JP, 11-328850, A (Sony Corporation), 30 November, 1999 (30.11.99) & WO, 99/59092, A1 & EP, 996074, A.	1-39

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
08 March, 2001 (08.03.01)

Date of mailing of the international search report
21 March, 2001 (21.03.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JP00/08497

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.
H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.
H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で利用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)
WPI (DIALOG)
INSPEC (DIALOG)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	Digital Transmission Content Protection Specification, Volume 1 (Informational Version), Revision 1.0, (1999 April)	1-39
EA	JP, 2000-357127, A (株式会社東芝) 26. 12月. 2000 (26. 12. 00), ファミリーなし	1-39

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

08. 03. 01

国際調査報告の発送日

21.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政



5W

9570

電話番号 03-3581-1101 内線 3574

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 6-326786, A (日立電子株式会社) 25. 11月. 1994 (25. 11. 94), ファミリーなし	1-39
A	JP, 11-328850, A (ソニー株式会社) 30. 11月. 1999 (30. 11. 99), & WO, 99/59092, A1 & EP, 996074, A	1-39

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.